ESET

REMOTE ADMINISTRATOR 5

Manual de instalação e guia do usuário

Clique aqui para fazer download da versão mais recente deste documento

ESET **REMOTE ADMINISTRATOR 5**

Copyright © 2014 **por ESET, spol. s r.o.**
ESET Remote Administrator 5 foi desenvolvido por ESET, spol. s r.o.
Para obter mais informações, visite www.eset.com.br.
Todos os direitos reservados. Nenhuma parte desta documentação pode ser reproduzida, armazenada em um sistema de recuperação ou transmitido de qualquer forma ou por qualquer meio, eletrônico, mecânico, fotocópia, gravação, digitalização, ou de outra forma sem a permissão por escrito do autor.
A ESET, spol. s r.o. reserva-se o direito de alterar qualquer software aplicativo descrito sem prévio aviso.

Atendimento ao cliente mundial: www.eset.eu/support
Atendimento ao cliente na América do Norte: www.eset.com/support

REV. 5/19/2014

Índice

1. Introdução 5
1.1 O que há de novo 5
1.2 Arquitetura do programa 7
2. Instalação do ERA Server e do ERA Console 8
2.1 Requisitos 8
2.1.1 Requisitos de software 8
2.1.2 Requisitos de desempenho 9
2.1.3 Portas usadas 11
2.2 Guia de instalação básica 13
2.2.1 Visão geral do ambiente (estrutura de rede) 13
2.2.2 Antes da instalação 14
2.2.3 Instalação 14
2.2.3.1 Instalação do ERA Server 14
2.2.3.1.1 Instalação no modo de agrupamento 15
2.2.3.2 Instalação do ERA Console 16
2.2.3.3 Imagem 16
2.2.3.4 Tipos de bancos de dados compatíveis com o ERA Server 17
2.2.3.4.1 Requisitos básicos 17
2.2.3.4.2 Configuração da conexão do banco de dados 18
2.2.3.5 Instalação em versões anteriores 18
2.3 Cenário - Instalação em um ambiente empresarial 20
2.3.1 Visão geral do ambiente (estrutura de rede) 20
2.3.2 Instalação 21
2.3.2.1 Instalação em sede 21
2.3.2.2 Filial: Instalação do ERA Server 21
2.3.2.3 Filial: Instalação do servidor de Imagem de HTTP 21
2.3.2.4 Filial: Instalação remota em clientes 21
2.3.3 Outros requisitos para ambientes empresariais 22
3. Trabalhar com o ERA Console 23
3.1 Conectando-se ao ERA Server 23
3.2 ERA Console - janela principal 24
3.2.1 Configuração de página 25
3.3 Filtragem de informações 25
3.3.1 Filtro 26
3.3.2 Menu de contexto 27
3.3.3 Filtro de data 27
3.4 Guias no ERA Console 28
3.4.1 Descrição geral de guias e clientes 28
3.4.2 Replicação e informações em guias individuais 29
3.4.3 Guia Clientes 29
3.4.4 Guia Log de ameaças 31
3.4.5 Guia Log do firewall 32
3.4.6 Guia Log de eventos 32
3.4.7 Guia Log do HIPS 32
3.4.8 Log de controle do dispositivo 33
3.4.9 Log de controle na Web 33
3.4.10 Guia Log de antispam 33
3.4.11 Guia Log da lista cinza 34
3.4.12 Guia Log de rastreamento 34
3.4.13 Guia Log de mobile 35
3.4.14 Guia Quarentena 35
3.4.15 Guia Tarefas 36
3.4.16 Guia Relatórios 36
3.4.16.1 Painel 38
3.4.16.1.1 Lista de servidores da web de painel 41
3.4.16.2 Cenário de relatório de exemplo 42
3.4.17 Guia Instalação remota 42
3.4.17.1 Assistente de tarefa de pesquisa de rede 43
3.4.17.2 Pacotes de instalação 44
3.4.17.3 Diagnóstico de instalação remota 46
3.4.17.4 Tarefas de instalação 47
3.5 Opções do ERA Console 48
3.5.1 Conexão 48
3.5.2 Colunas 48
3.5.3 Cores 49
3.5.4 Caminhos 49
3.5.5 Data/hora 49
3.5.6 Outras configurações 49
3.6 Modos de exibição 50
3.7 Editor de configuração da ESET 50
3.7.1 Camadas de configuração 51
3.7.2 Principais entradas de configuração 52
4. Instalação de soluções clientes da ESET 53
4.1 Instalação direta 53
4.2 Instalação remota 53
4.2.1 Requisitos 54
4.2.1.1 Requisitos para instalação forçada de Linux/Mac 55
4.2.2 Instalação forçada remota 55
4.2.3 Instalação remota por logon/email 57
4.2.3.1 Exportar instalador da ESET para pasta/script de logon 58
4.2.3.2 Logon padrão 59
4.2.4 Instalação remota personalizada 60
4.2.5 Cliente de atualização 61
4.2.6 Evitando instalações repetidas 61
4.3 Instalação em um ambiente empresarial 62
5. Administrando computadores clientes 64
5.1 Tarefas 64
5.1.1 Tarefa de configuração 65
5.1.2 Tarefa de rastreamento sob demanda 65
5.1.3 Tarefa Atualizar agora 66
5.1.4 Tarefa de script do SysInspector 66
5.1.5 Recursos de proteção 66
5.1.6 Executar tarefa agendada 67
5.1.7 Restaurar/excluir da tarefa de quarentena 67
5.1.8 Reversão de banco de dados de vírus 67
5.1.9 Limpar cache de atualização do cliente 68
5.1.10 Gerar tarefa de log de auditoria de segurança 68
5.1.11 Mostrar tarefa de notificação 68
5.1.12 Concluindo a tarefa 68
5.2 Gerenciador de grupos 69
5.2.1 Grupos estáticos 69
5.2.2 Grupos paramétricos 70
5.2.3 Sincronização do Active Directory / LDAP 70
5.3 Políticas 71
5.3.1 Princípios básicos e operação 71
5.3.2 Como criar políticas 71
5.3.3 Políticas virtuais 72
5.3.4 Função e finalidade de políticas na estrutura em árvore de política 72
5.3.5 Visualizando políticas 73
5.3.6 Importando/exportando políticas 73
5.3.7 Assistente de migração de política 73
5.3.8 Atribuindo políticas a clientes 74
5.3.8.1 Política de clientes primários padrão 74
5.3.8.2 Atribuição manual 74
5.3.8.3 Regras de política 74
5.3.8.3.1 Assistente de regras de política 75
5.3.9 Políticas para clientes móveis 76
5.3.10 Excluindo políticas 76
5.3.11 Configurações especiais 77
5.3.12 Cenários de implantação de política 78
5.3.12.1 Cada servidor é uma unidade autônoma e as políticas são definidas localmente 78
5.3.12.2 Cada servidor é administrado individualmente - as políticas são gerenciadas localmente, mas a Política pai padrão é herdada do servidor superior 79
5.3.12.3 Herdando políticas de um servidor superior 80
5.3.12.4 Atribuindo políticas somente do servidor superior 81
5.3.12.5 Usando grupos 81
5.4 Gerenciador de notificações 82
5.4.1 Estado de cliente 84

5.4.2 Estado de servidor ... 86
5.4.3 Evento de tarefa concluído ... 87
5.4.4 Novo evento de cliente ... 87
5.4.5 Evento de epidemia ... 88
5.4.6 Evento de log recebido ... 88
5.4.7 Ação ... 89
5.4.8 Notificações via Interceptação SNMP ... 90
5.4.9 Exemplo de criação de regras ... 90
5.5 Informações detalhadas de clientes ... 90
5.6 Assistente de fusão de regras de firewall ... 91
6. Opções do ERA Server ... 92
6.1 Geral ... 92
6.1.1 Gerenciamento de licenças ... 92
6.2 Segurança ... 93
6.2.1 Gerenciador de usuários ... 94
6.2.2 Senha de acesso ao console ... 94
6.3 Manutenção do servidor ... 94
6.3.1 Parâmetros de coleta de log ... 95
6.3.2 Limpeza por parâmetro de tempo ... 95
6.3.3 Configurações avançadas de limpeza por contagem de registros de log ... 96
6.4 Registro em log ... 96
6.4.1 Visualizador do log de auditoria ... 98
6.5 Replicação ... 98
6.5.1 Replicação em grandes redes ... 99
6.6 Atualizações ... 101
6.6.1 Servidor de imagem ... 102
6.6.1.1 Operação do servidor de imagem ... 103
6.6.1.2 Tipos de atualizações ... 103
6.6.1.3 Como ativar e configurar a Imagem ... 104
6.7 Outras configurações ... 105
6.8 Avançadas ... 105
7. Console da linha de comando ERA ... 107
7.1 Sinalizadores de comando ... 109
7.2 Comandos ... 110
8. ERA Maintenance Tool ... 128
8.1 Parar o ERA Server ... 128
8.2 Iniciar o ERA Server ... 128
8.3 Transferência do banco de dados ... 129
8.4 Backup do banco de dados ... 129
8.5 Restauração do banco de dados ... 130
8.6 Excluir tabelas ... 130
8.7 Backup de armazenamento ... 130
8.8 Restauração de armazenamento ... 130
8.9 Instalar nova chave de licença ... 131
8.10 Modificar configuração do servidor ... 131
8.11 Interface da linha de comando ... 131
9. Solução de problemas ... 132
9.1 FAQ ... 132
9.1.1 Problemas com a instalação do ESET Remote Administrator no Windows Server 2000/2003 ... 132
9.1.2 Qual é o significado do código de erro GLE? ... 132
9.2 Códigos de erros frequentemente encontrados ... 132
9.2.1 Mensagens de erro exibidas ao usar o ESET Remote Administrator para instalar remotamente o ESET Smart Security ou o ESET NOD32 Antivirus ... 132
9.2.2 Códigos de erros frequentemente encontrados no era.log ... 133
9.3 Como diagnosticar problemas com o ERAS? ... 133
10. Sugestões e dicas ... 135
10.1 Agenda ... 135
10.2 Removendo perfis existentes ... 136
10.3 Exportação e outros recursos da configuração XML do cliente ... 137
10.4 Atualização combinada para notebooks ... 137
10.5 Instalação de produtos de terceiros usando o ERA ... 138
11. ESET SysInspector ... 140
11.1 Introdução ao ESET SysInspector ... 140
11.1.1 Iniciando ESET SysInspector ... 140
11.2 Interface do usuário e uso do aplicativo ... 141
11.2.1 Controles do programa ... 141
11.2.2 Navegação no ESET SysInspector ... 142
11.2.2.1 Atalhos do teclado ... 143
11.2.3 Comparar ... 145
11.3 Parâmetros da linha de comando ... 146
11.4 Script de serviços ... 146
11.4.1 Geração do script de serviços ... 146
11.4.2 Estrutura do script de serviços ... 147
11.4.3 Execução de scripts de serviços ... 149
11.5 FAQ ... 150
12. ESET SysRescue ... 152
12.1 Requisitos mínimos ... 152
12.2 Como criar o CD de restauração ... 152
12.3 Seleção de alvos ... 153
12.4 Configurações ... 153
12.4.1 Pastas ... 153
12.4.2 Antivírus ESET ... 154
12.4.3 Configurações avançadas ... 154
12.4.4 Protoc. Internet ... 154
12.4.5 Dispositivo USB inicializável ... 154
12.4.6 Gravar ... 155
12.5 Trabalhar com o ESET SysRescue ... 155
12.5.1 Utilização do ESET SysRescue ... 155
13. Apêndice - Licença de terceiros ... 156

1. Introdução

O ESET Remote Administrator (ERA) é um aplicativo que permite que você gerencie produtos da ESET em um ambiente de rede, incluindo estações de trabalho e servidores - de um local central. Com o sistema de gerenciamento de tarefas incorporado do ESET Remote Administrator, você poderá instalar soluções de segurança da ESET em computadores remotos e responder rapidamente a novos problemas e ameaças.

O ESET Remote Administrator por si só não fornece qualquer outra forma de proteção em relação a código malicioso. O ERA depende da presença de uma solução de segurança da ESET em estações de trabalho ou servidores, como ESET NOD32 Antivirus ou ESET Smart Security.

Para realizar uma implantação completa de um portfólio de soluções de segurança da ESET, as seguintes etapas devem ser realizadas:

- Instalação do ERA Server (ERAS),
- Instalação do ERA Console (ERAC),
- Instalação em computadores clientes (ESET NOD32 Antivirus, ESET Smart Security, etc...).

OBSERVAÇÃO: algumas partes deste documento usam variáveis do sistema que se referem a um local exato de pastas e arquivos:

%ProgramFiles% = geralmente *C:\Program Files*
%ALLUSERSPROFILE% = geralmente *C:\Documents and Settings\All Users*

1.1 O que há de novo

ESET Remote Administrator versão 5.0

Novos recursos

- Web Dashboard para administradores - visão geral abrangente de relatórios em seu navegador
- Instalação remota - novo design
- Recursos de proteção - nova tarefa para o gerenciamento de recursos de proteção em clientes
- Executar tarefa agendada - nova tarefa para acionar imediatamente uma tarefa agendada em um cliente
- Gerenciador de usuários - ferramenta para o gerenciamento de contas e senhas para acesso ao console
- Guia HIPS - informações sobre eventos relacionados ao HIPS de clientes
- Guia Controle na Web - informações sobre eventos relacionados ao Controle na Web de clientes
- Guia Controle de dispositivo - informações sobre eventos relacionados ao Controle de dispositivo de clientes
- Guia Antispam - informações sobre eventos relacionados ao spam de clientes
- Guia Lista cinza - informações sobre eventos relacionados à lista cinza de clientes
- Pesquisa de computadores na rede - novas tarefas de pesquisa e design
- Suporte à instalação em versões anteriores do ERA (4.x, 3.x), incluindo migração de dados
- Relatórios - novos relatórios, novo design, suporte para web dashboards

ESET Remote Administrator versão 4.0

- Suporte para ESET Smart Security/ESET NOD32 Antivirus 4.2
- Suporte para ESET Mail Security 4 for Microsoft Exchange Server
- Suporte para ESET Mobile Security

Novos recursos

- Instalação remota - novo design
- Gerenciamento de grupos - novo design (Grupos estáticos, Grupos paramétricos, sincronização aprimorada do Active Directory)
- Filtro - funcionalidade aprimorada (filtros de política, filtros de grupos estáticos e paramétricos)
- Políticas - novos parâmetros em regras de política (suporte para grupos paramétricos), importação/exportação de políticas e regras de política, fusão de tarefas da agenda, assistente de regras de política
- Notificações - suporte para grupos paramétricos + várias melhorias pequenas
- Visão centralizada de quarentena de clientes (para clientes ESS/EAV v4 e superiores)
- Relatórios - suporte para grupos estáticos e paramétricos, novos tipos de relatórios (log de mobile, quarentena, firewall), novos modelos
- Assistente de fusão de regras de firewall - assistente para fusão de regras criadas no modo de aprendizado
- Autenticação do Windows/domínio de usuários do ERA Console
- Suporte a agrupamento passivo do Windows
- Suporte à instalação em versões anteriores do ERA (3.x, 2.x, 1.x), incluindo migração de dados
- Criptografia de comunicação com o AES-256

Novo Editor de configuração da ESET

- Suporte para novos produtos de segurança da ESET
- Suporte para novos recursos do ERA Server
- Arquivos de licença compactados
- Capacidade de adicionar tarefas agendadas predefinidas

ESET Remote Administrator versão 3.0

- Suporte para produtos de segurança da ESET 4.x
- Suporte para soluções Linux

Novos recursos

- Gerenciamento de políticas
- Gerenciador de notificações
- Acesso somente leitura ao console
- Suporte para ESET SysInspector
- Escalabilidade aprimorada de transferência de dados
- Exclusão de clientes replicados
- Fusão de chave de licença/Gerenciador de licenças
- Imagem para ESET NOD32 Antivirus 2.x
- Nova configuração
- Opção de filtragem baseada em domínio adicionada na localização de computadores não registrados
- Compactação de logs de servidor (zip)
- Bugs pequenos corrigidos e vários recursos pequenos adicionados
- CD de restauração

Melhorias no servidor interno

- Suporte para bancos de dados adicionais (MS Access, MS SQL Server, Oracle, MySQL)

Novo Editor de configuração da ESET

- Suporte para produtos de segurança da ESET 4.x

ESET Remote Administrator versão 2.0

- Suporte para novos produtos de segurança da ESET 3 (ESET Smart Security, ESET NOD32 Antivirus)
- Novos logs (novas colunas, logs do ESET Personal Firewall)
- Novas informações de status de cliente para clientes versão 3 (status de proteção, recursos de proteção, informações do sistema)
- Tarefas (configuração, atualizar agora, rastreamento sob demanda, tarefa interativa)
- Ainda é compatível com produtos NOD32 versão 2.x

Novos recursos

- Identificação de cliente estendida (endereço MAC adicionado)
- Instalação remota estendida (suporte a pacotes msi e personalizados)
- Melhorias de segurança (capacidade de criptografia para todos os novos clientes de servidor)

- Melhorias em desempenho (compactação no protocolo de comunicação)
- Acréscimo de encaminhamento de dados do ESET Live Grid via ERA Server
- Melhorias na GUI (novos gráficos, cor de status aprimorada, filtros estendidos, caixas de diálogo redimensionáveis)
- Novo modelo de relatório (esquema ESS)
- Monitoramento de desempenho do servidor (dados, consultas)
- Funcionalidade de atualização no ERA Server (permite a atualização de informações importantes)
- Funcionalidade de imagem no ERA Server
- Instalação remota estendida (suporte de pacotes msi e personalizados, instalação remota do ERA, diagnóstico)

Melhorias no servidor interno

- Replicação aprimorada (prioridade de replicação, replicação melhor em vários níveis)
- Nova estrutura de banco de dados
- Nova estrutura de diretório
- Melhorias em segurança interna

Novo Editor de configuração da ESET

- Suporte a produtos de segurança da ESET, versão 2 e versão 3
- Capacidade de configurar o ERA Server
- Outros recursos novos menores (configurações personalizadas e de pesquisa)

Novo instalador (MSI)

- Migração de banco de dados de versões anteriores
- Nova documentação (ajuda, manual)

1.2 Arquitetura do programa

Tecnicamente, o ESET Remote Administrator consiste em dois componentes separados: ERA Server (ERAS) e ERA Console (ERAC). Você pode executar um número ilimitado de ERA Servers e Consoles em sua rede, pois não há limitações no contrato de licença para seu uso. A única limitação é o número total de clientes que sua instalação do ERA pode administrar.

ERA Server (ERAS)

O componente de servidor do ERA é executado como um serviço nos seguintes sistemas operacionais baseados em Microsoft Windows® NT: 2000, XP, 2003, Vista, 7 e 2008. A principal tarefa desse serviço é coletar informações de clientes e enviá-las para várias solicitações. Essas solicitações, incluindo tarefas de confirmação, solicitações de instalação remota, são criadas através do ERA Console (ERAC). O ERAS é um ponto de encontro entre o ERAC e computadores clientes - um local onde todas as informações são processadas, mantidas ou modificadas antes de serem transferidas para clientes ou para o ERAC.

ERA Console (ERAC)

O ERAC é o componente cliente do ERA e geralmente está instalado em uma estação de trabalho. Essa estação de trabalho é usada pelo administrador para controlar remotamente soluções da ESET em clientes individuais. Usando o ERAC, o administrador pode conectar-se ao componente de servidor do ERA - na porta TCP 2223. A comunicação é controlada pelo processo console.exe, que geralmente está localizada no seguinte diretório:

%ProgramFiles%\ESET\ESET Remote Administrator\Console

Ao instalar o ERAC, talvez seja preciso inserir o nome de um ERAS. Mediante a inicialização, o console se conectará automaticamente a esse servidor. O ERAC também pode ser configurado depois da instalação.

2. Instalação do ERA Server e do ERA Console

2.1 Requisitos

O ERAS funciona como um serviço e, portanto, exige um sistema operacional baseado em Microsoft Windows NT (2000, XP, 2003, Vista, 7 ou 2008). Embora o Microsoft Windows Server Edition não seja necessário para que o ERAS funcione, recomendamos a instalação do ERAS em sistemas operacionais baseados em servidor para o seu perfeito funcionamento. Um computador com o ERAS instalado nele deve sempre estar on-line e acessível através da rede do computador por:

- Clientes (geralmente estações de trabalho)
- PC com ERA Console
- Outras instâncias do ERAS (se replicado)

OBSERVAÇÃO: o ESET Remote Administrator 5 é compatível com a instalação em versões anteriores 18, incluindo migração de dados.

2.1.1 Requisitos de software

ERA Server

Sistemas operacionais de 32 bits:	Windows 2000 e versões posteriores (ver **Observação**)
Sistemas operacionais de 64 bits:	Windows XP e versões posteriores
Bancos de dados:	Microsoft Access (incorporado) Microsoft SQL Server 2005 e versões posteriores MySQL 5.0 e versões posteriores ORACLE 9i e versões posteriores
Windows Installer:	2.0 e versões posteriores
Web Dashboard:	Internet Explorer 7.0 e versões posteriores Mozilla Firefox 3.6 e versões posteriores Google Chrome 9 e versões posteriores
Servidor HTTP (HTTP Server):	Mesmo que os requisitos do ERA Server, mas requer SP2 e versões posteriores no Windows XP

ERA Console

Sistemas operacionais de 32 bits:	Windows 2000 e versões posteriores (ver **Observação**)
Sistemas operacionais de 64 bits:	Windows XP e versões posteriores
Windows Installer:	2.0 e versões posteriores
Internet Explorer:	7.0 e versões posteriores

Observação:

- o ERA Console não é compatível com Microsoft Windows Server Core 2008 e Microsoft Windows Server Core 2012. O ERA Server é compatível nestes sistemas operacionais, mas não será compatível com a integração com o Microsoft Access Database.
- Para iniciar o ERA Console, o Editor de Configuração ESET e a Ferramenta de Manutenção ERA no Windows 2000, você precisa do arquivo *gdiplus.dll* no seu sistema. Você pode baixar este arquivo aqui. Extraia o arquivo do pacote de instalação e copie-o para o diretório *C:\WINNT\system32*.
- O papel do HTTPS Server não é compatível com o Windows 2000, portanto, as funções Dashboard e Mirror não funcionarão no modo HTTPS neste sistema operacional. Para usar o recurso Dashboard em um servidor Windows

2000, edite as configurações de modo que o Dashboard não seja executado no modo HTTPS como padrão.

- A instalação remota para produtos de segurança Linux/MAC não é compatível com Windows 2000.
- Alguns sistemas operacionais vão precisar que você atualize os certificados confiáveis de raiz antes de uma instalação forçada ser realizada com sucesso. É possível atualizar esses certificados executando o serviço Windows Update ou manualmente, importando as versões mais recentes.
- Se você usar uma conta de administrador para configurar o acesso SMTP em **Ferramentas** > **Opções de servidor** > **Outras configurações** (para IIS ou Exchange), a saída de email pode não funcionar.
- Algumas funções (RDP, Shutdown) das **Ações de rede** (descritas na seção Guia Clientes 291) não estão disponíveis no Windows 2000.

2.1.2 Requisitos de desempenho

O desempenho do servidor pode variar dependendo dos seguintes parâmetros:

1. Banco de dados usado

- Banco de dados MS Access - por padrão, instalado com o servidor. Recomendamos essa solução ao atender centenas de clientes. No entanto, há um limite de tamanho de 2 GB para o banco de dados. Consequentemente, você precisará ativar limpezas no servidor e definir um intervalo (em **Ferramentas** > **Opções do servidor** > **Manutenção do servidor**) para remover dados antigos.
- Outros bancos de dados (MySQL, MSSQL, ORACLE) exigem uma instalação separada, mas podem resultar em desempenho melhor. É essencial usar hardware adequado para cada mecanismo de banco de dados (principalmente ORACLE) seguindo as recomendações técnicas de seu distribuidor.
- Se escolher a ORACLE como sua solução de banco de dados, você deve definir o número de cursores acima do valor **Número máximo de conexões ativas** (em **Ferramentas** > **Opções do servidor** > **Avançadas** > **Editar configurações avançadas** > **Avançadas**; o padrão é definido como 500). O número final de cursores deve considerar o número de servidores inferiores (se a replicação for usada) e cursores que são usados por outros aplicativos acessando o mecanismo de banco de dados.
- Geralmente, o desempenho do servidor é superior ao usar bancos de dados externos (ou seja, instalados em outra máquina física).

2. Configurações de intervalo de conexão do cliente

- O intervalo de conexão do cliente é definido como 10 minutos por padrão em ESET Smart Security/ESET NOD32 Antivirus versões 4.2 e posteriores. Se precisar do status do cliente para atualizar mais ou menos frequentemente do que o intervalo padrão, você poderá modificar essa configuração. Lembre-se de que um intervalo de conexão do cliente menor afetará o desempenho do servidor.

3. Número médio de eventos reportados pelos clientes por conexão

- Qualquer informação enviada do cliente para o servidor será relacionada no evento especificado (por exemplo, log de ameaça, log de evento, log de rastreamento ou alteração de configuração). Esse parâmetro não pode ser alterado diretamente, mas pode ser alterado se outras configurações relevantes para ele forem alteradas. Por exemplo, em configuração avançada do servidor (em **Ferramentas** > **Opções do servidor** > **Manutenção do servidor**), você pode configurar a quantidade máxima de logs que podem ser aceitos pelo servidor (essa configuração inclui clientes que se conectam diretamente, bem como clientes replicados). Em operações regulares, a média a longo prazo pode ser estimada em 1 evento a cada 4 horas por cliente.

4. Hardware usado

Para **instalações pequenas (menos de 1.000 clientes conectando-se ao ERA Server):**

- Tipo de processador - processador compatível com Pentium IV, 2,0 GHz ou superior
- RAM - 2 GB
- Rede - 1 gigabit

Para **instalações médias (de 1.000 a 4.000 clientes conectando-se ao ERA Server),** recomendamos dividir a instalação em dois computadores:

ERA Server:

- Tipo de processador - processador compatível com Pentium IV, 2,0 GHz ou superior
- RAM - 2 GB
- Rede - 1 gigabit

Servidor do banco de dados:

- Tipo de processador - processador compatível com Pentium IV, 2,0 GHz ou superior
- RAM - 2 GB
- Rede - 1 gigabit

Ou você pode instalar o ERA Server e o banco de dados em um computador:

- Tipo de processador - processador compatível com Pentium IV, vários núcleos, 3,0 GHz ou superior
- RAM - 4 GB
- Rede - 1 gigabit
- HDD - unidade de disco rígido Raid 0 ou SSD ou ambas

OBSERVAÇÃO: nesse caso (o ERA Server e o banco de dados instalados em um computador), não recomendamos o banco de dados MS Access, pois seu limite de tamanho de 2 GB necessita de limpezas regulares de banco de dados. Além disso, lembre-se de que o banco de dados MS SQL Express tem um limite de tamanho de apenas 4 GB.

Para **instalações grandes (de 4.000 a 10.000 clientes conectando-se ao ERA Server),** recomendamos dividir as instalações em 2 computadores e usar o banco de dados MS SQL ou Oracle:

ERA Server:

- Tipo de processador - processador compatível com Pentium IV, vários núcleos, 3,0 GHz ou superior
- RAM - 4 GB
- Rede - 1 gigabit

Servidor do banco de dados:

- Tipo de processador - processador compatível com Pentium IV, vários núcleos, 3,0 GHz ou superior
- RAM - 4 GB
- Rede - 1 gigabit
- HDD - unidade de disco rígido Raid 0 ou SSD ou ambas

Para instalações extragrandes (de 10.000 a 20.000 clientes em um ERA Server), recomendamos dividir as instalações em 2 computadores e usar o banco de dados MS SQL ou Oracle:

ERA Server:

- Tipo de processador - processador compatível com Pentium IV, vários núcleos, 3,0 GHz ou superior
- RAM - 8 GB
- Rede - 1 gigabit
- HDD - unidade de disco rígido Raid 0 ou SSD ou ambas

Servidor do banco de dados:

- Tipo de processador - processador compatível com Pentium IV, vários núcleos, 3,0 GHz ou superior
- RAM - 4 GB
- Rede - 1 gigabit
- HDD - unidade de disco rígido Raid 0 ou SSD ou ambas

OBSERVAÇÃO: todas as configurações de hardware relacionadas acima representam os requisitos mínimos para execução do ERA. Recomendamos usar configurações melhores para ter melhor desempenho. Recomendamos que você use o hardware mínimo recomendado para seu sistema operacional de servidor ao considerar o número de clientes a serem atendidos. Para obter mais informações sobre os tipos de bancos de dados usados e seus limites, consulte o capítulo intitulado Tipos de bancos de dados compatíveis com o ERA Server 17.

Sobrecarga

Se um servidor estiver sobrecarregado (p. ex., ao conectar 20.000 clientes em um servidor capaz de atender apenas a 10.000 clientes em um intervalo de cada 10 minutos), ele ignorará alguns dos clientes conectados. Em média, a cada segundo a conexão de cliente será atendida, pois se o intervalo de conexão de cliente foi definido em 20 minutos em vez de 10. Cada negação de serviço será registrada da seguinte forma: "*<SERVERMGR_WARNING> ServerThread: o número máximo de encadeamentos para conexões ativas foi atingido (500), o servidor ignorará essa conexão*". As negações de serviço também podem ocorrer durante sobrecargas temporárias do servidor.

Você pode alterar o valor na opção **Número máximo de conexões ativas** (o padrão é 500) nas configurações avançadas do servidor, mas recomendamos fazer isso somente em casos excepcionais (por exemplo, ao resolver problemas específicos). Caso haja uma superabundância de recursos de sistema e desempenho de mecanismo do banco de dados, você poderá usar essa configuração para ajustar o desempenho geral do servidor.

Transferência de dados em uma rede

Durante a operação padrão do servidor, podemos estimar que uma conexão de cliente a cada 10 minutos reportará 0,04 evento por conexão, que é 1 evento reportado a cada 4 horas por cliente. Isso produzirá aproximadamente 2 quilobytes de tráfego por conexão.

Em um cenário de epidemia de vírus, com um cliente reportando 7 eventos sempre que se conectar, o tráfego poderá aumentar para até 240 quilobytes por conexão. Se você usar a compactação (padrão), os dados transferidos serão aproximadamente 50% menores em tamanho, ou seja, em torno de 120 quilobytes por conexão.

Os dados incluem conexões diretas de cliente e omite conexões replicadas. A replicação ocorre muito menos frequentemente e os servidores enviam novos eventos de servidores inferiores. O nível de detalhamento de eventos replicados automaticamente pode ser configurado nas configurações avançadas do servidor (em **Ferramentas** > **Opções do servidor** > **Avançadas** > **Editar configurações avançadas** > **Replicação**). Na seção Manutenção do servidor, você pode configurar o nível máximo de logs que o servidor superior aceitará (essa configuração aplica-se somente a clientes conectando-se diretamente e clientes replicados).

Requisitos de capacidade de armazenamento

A instalação limpa do ESET Remote Administrator com um banco de dados MS Access requer até 60 MB de espaço em disco.

A maioria do espaço de armazenamento é usado por eventos de clientes que são armazenados no banco de dados e em um repositório no disco (o diretório padrão é *C:\Documents and Settings\All Users\Application Data\Eset\ESET Remote Administrator\Server*). O ERA requer que, pelo menos, 5% do disco esteja livre. Se esse mínimo for excedido, o servidor parará de receber alguns dos eventos do cliente. Essa configuração pode ser encontrada em **Ferramentas** > **Opções do servidor** > **Avançadas** > **Editar configurações avançadas** > **Avançadas** > **Uso máximo de espaço em disco**. Aproximadamente 10 GB por 1.000 clientes de espaço livre em disco são necessários para operação regular nas configurações de limpeza padrão (excluir eventos anteriores a 3 meses).

Estudo de caso

Um servidor usando um banco de dados MS Access que tem clientes conectando-se a cada 5 minutos e reportando 7 eventos (p. ex., log de ameaça, log de evento, log de rastreamento, alteração de configuração, etc.) por conexão, em média, pode atender temporariamente a 3.000 clientes. Esse cenário descreve uma situação de sobrecarga temporária, como geração de relatórios durante uma epidemia de vírus.

Se o servidor usar um banco de dados MySQL externo e o intervalo da conexão do cliente for definido como 10 minutos (gerando 0,02 eventos por conexão em média), o número máximo de clientes que o servidor poderá atender aumenta para 30.000. Esse cenário mostra desempenho de banco de dados ideal, com clientes reportando um número relativamente pequeno de eventos.

Na operação normal, usar um banco de dados MS Access e um intervalo de conexão do cliente de 10 minutos permitirá que o servidor atenda a um máximo de 10.000 clientes.

2.1.3 Portas usadas

O gráfico a seguir relaciona as possíveis comunicações de rede usadas quando o ERAS está instalado. O processo EHttpSrv.exe realiza a escuta na porta TCP 2221 e o processo era.exe realiza a escuta nas portas TCP 2222, 2223, 2224 e 2846. Outras comunicações ocorrem com o uso de processos de sistema operacional nativo (p. ex., "NetBIOS em TCP/IP").

Protocolo	Porta	Descrição
TCP	2221 (ERAS na escuta)	Porta padrão usada pelo recurso de Imagem integrado no ERAS (versão HTTP)
TCP	2222 (ERAS na escuta)	Comunicação entre clientes e o ERAS
TCP	2223 (ERAS na escuta)	Comunicação entre o ERAC e o ERAS

Para que todos os recursos do programa funcionem devidamente, certifique-se de que as seguintes portas de rede estejam abertas:

Protocolo	Porta	Descrição
TCP	2224 (ERAS na escuta)	Comunicação entre o agente *einstaller.exe* e o ERAS durante a instalação remota
TCP	2225 (ERAS na escuta)	Comunicação entre o ESET Dashboard HTTP Server e o ERAS
TCP	2846 (ERAS na escuta)	Replicação do ERAS.
TCP	139 (porta de destino da perspectiva do ERAS)	Cópia do agente *einstaller.exe* do ERAS para um cliente usando o compartilhamento admin$
UDP	137 (porta de destino da perspectiva do ERAS)	"Resolução de nome" durante a instalação remota.
UDP	138 (porta de destino da perspectiva do ERAS)	"Procura" durante a instalação remota
TCP	445 (porta de destino da perspectiva do ERAS)	Acesso direto a recursos compartilhados usando TCP/IP durante a instalação remota (uma alternativa para TCP 139)

As portas predefinidas 2221, 2222, 2223, 2224, 2225 e 2846 podem ser alteradas se já tiverem sido usadas por outros aplicativos.

Para alterar as portas padrão usadas pelo ERA, clique em **Ferramentas** > **Opções do servidor...**. Para alterar a porta 2221, selecione a guia **Atualizações** e altere o valor de porta do servidor HTTP. As portas 2222, 2223, 2224, 2225 e 2846 podem ser modificadas na seção **Portas** da guia Outras configurações 105.

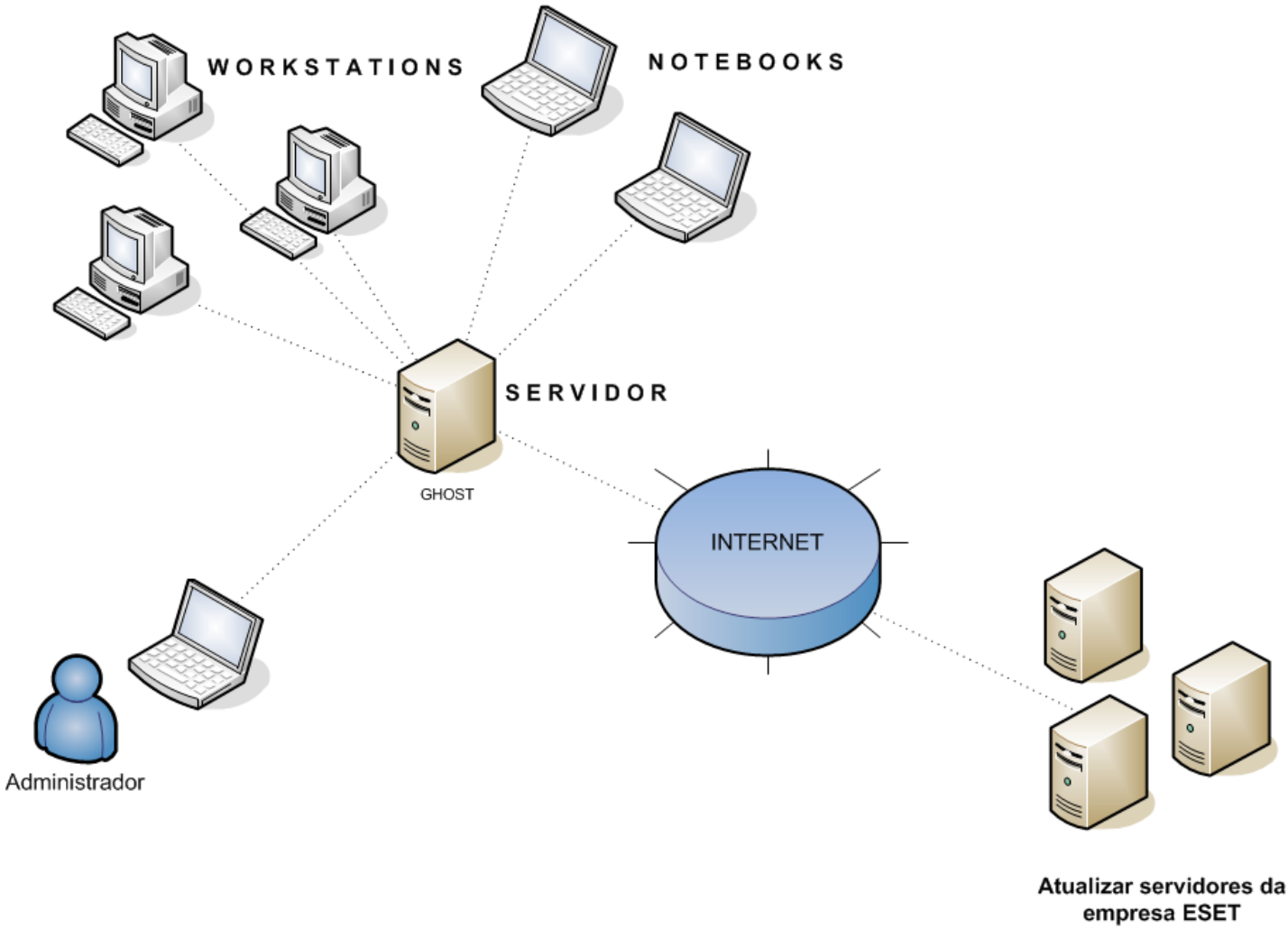
As portas predefinidas 2222, 2223, 2224 e 2846 também podem ser modificadas usando o modo de instalação avançada (ERAS).

2.2 Guia de instalação básica

2.2.1 Visão geral do ambiente (estrutura de rede)

A rede de uma empresa geralmente consiste em uma rede de área local (LAN); portanto, sugerimos instalar um ERAS e um servidor de imagem. O servidor de imagem pode ser criado no ERAS ou no ESET NOD32 Antivirus Business Edition/ ESET Smart Security Business Edition.

Suponha que todos os clientes sejam notebooks e estações de trabalho com Microsoft Windows 2000/XP/Vista/7, colocados em rede em um domínio. O servidor denominado GHOST está on-line 24 horas por dia, nos sete dias da semana, e pode ser uma estação de trabalho com Windows, Professional ou Server Edition (não precisa ser um servidor com Active Directory). Além disso, suponha que notebooks não estão presentes na rede da empresa durante a instalação de soluções clientes da ESET. A estrutura de rede pode ser semelhante a esta:



2.2.2 Antes da instalação

Antes da instalação, os seguintes pacotes de instalação devem ser baixados do site da ESET:

Componentes do ESET Remote Administrator:

ESET Remote Administrator - servidor
ESET Remote Administrator - console

Soluções clientes da ESET:

ESET Endpoint Security
ESET Endpoint Antivirus
ESET Smart Security 4.x
ESET Smart Security 3.x
ESET NOD32 Antivirus 4.x
ESET NOD32 Antivirus 3.x
ESET NOD32 Antivirus 2.7

OBSERVAÇÃO: baixe as soluções clientes que você usará em estações de trabalho clientes.

2.2.3 Instalação

2.2.3.1 Instalação do ERA Server

Instale o ERAS no servidor nomeado GHOST (veja o exemplo na Visão geral do ambiente 13). Para iniciar, selecione os componentes que deseja instalar. Há duas opções, **ESET Remote Administrator Server** e **ESET HTTP Dashboard 38 Server**.

Para a maioria dos aplicativos, ambos os componentes serão instalados. Você poderá escolher instalar os dois componentes em diferentes computadores (por exemplo, instalar o ESET HTTP Dashboard Server em um computador visivelmente público ao instalar o ERAS em um computado que esteja acessível somente de uma intranet local). Ou você pode escolher não usar o ESET HTTP Dashboard Server.

OBSERVAÇÃO: recomendamos instalar o ERAS em uma máquina executando um sistema operacional de servidor.

OBSERVAÇÃO: o servidor de imagem e o Dashboard usam o mesmo servidor HTTP (que é instalado automaticamente). Portanto, mesmo se desmarcar o servidor Dashboard no momento da instalação, você poderá habilitá-lo posteriormente no 'ESET Configuration Editor' (**ERAC** > **Ferramentas** > **Opções do servidor** > **Avançadas** > **Dashboards** > **Usar dashboard local**).

Depois de escolher os componentes desejados, selecione o modo de instalação **Típica** ou **Avançada**.

- Se você selecionar o modo **Típica**, o programa solicitará que você insira uma chave de licença (um arquivo com a extensão .lic ou .zip), que autorizará a operação do ERAS pelo período definido na licença. Em seguida, o programa pedirá que você defina os parâmetros de atualização (nome de usuário, senha e servidor de atualização). Você também poderá prosseguir para a próxima etapa e inserir os parâmetros de atualização posteriormente marcando a caixa de seleção ao lado de **Definir parâmetros de atualização posteriormente** e clicando em **Avançar**.
- Selecionar **Modo de instalação avançada** permitirá que você configure parâmetros de instalação adicionais. Esses parâmetros poderão ser modificados posteriormente através do ERAC, mas na maioria dos casos isso não será necessário. A única exceção é o nome do servidor, que deve corresponder ao nome DNS ou ao valor %COMPUTERNAME% de seu sistema operacional, ou ao endereço IP atribuído ao computador. Essa é a parte mais importante de informação para realizar uma instalação remota. Se um nome não for especificado durante a instalação, o instalador fornecerá automaticamente o valor da variável do sistema %COMPUTERNAME%, que é suficiente na maioria dos casos. Além disso, é importante selecionar o banco de dados no qual as informações do ERAS serão armazenadas. Para obter mais informações, consulte o capítulo intitulado Tipos de bancos de dados compatíveis com o ERA Server 17.

OBSERVAÇÃO: Ao instalar o ERAS em um sistema operacional Windows 2000, não recomendamos usar o DNS; use a cadeia de conexão completa.

Importante: As políticas de segurança do Microsoft Windows limitam permissões de conta de usuário local. Como uma consequência, você pode não conseguir executar operações de rede relacionadas. Executar o serviço ERA em uma conta de usuário local pode resultar em problemas de instalação forçada (p. ex., ao instalar remotamente do domínio para o grupo de trabalho). Ao usar o Windows Vista, Windows Server 2008 ou Windows 7, recomendamos o uso do serviço ERA em contas com direitos de rede suficientes. Você poderá especificar a conta de usuário na qual você deseja

executar o ERA no **modo de instalação avançada**.

Observação: embora o ERA Server seja totalmente compatível com Unicode, há situações em que o servidor converte caracteres em ANSI ou vice-versa (por exemplo, email, nome de computador). Em tais situações, a configuração **Idioma para programas não Unicode** deverá ser usada. Recomendamos que altere essa configuração para corresponder à localidade do ambiente do servidor se você não estiver usando uma versão localizada do ERA (ou seja, estiver usando a mutação do idioma inglês). Você poderá encontrar essa configuração em **Painel de controle** > **Opções regionais e de idioma** na guia **Avançadas**.

Os componentes do programa ERAS são instalados por padrão no seguinte diretório:

%ProgramFiles%\ESET\ESET Remote Administrator\Server

Outros componentes de dados, como logs, pacotes de instalação, configuração, etc., são armazenados no seguinte diretório:

%ALLUSERSPROFILE%\Application Data \ESET\ESET Remote Administrator\Server

O ERAS será iniciado automaticamente depois da instalação. A atividade do serviço ERAS é registrada no seguinte local:

%ALLUSERSPROFILE%\Application Data\ESET\ESET Remote Administrator\Server\logs\era.log

Instalação da linha de comando

O ERAS pode ser instalado usando os seguintes parâmetros da linha de comando:

/q - instalação silenciosa. Nenhuma intervenção do usuário é possível. Não são exibidas janelas de caixa de diálogo.

/qb - não é possível intervenção do usuário, mas o progresso de instalação é indicado pela barra de progresso.

Exemplo: *era_server_nt32_ENU.msi /qb*

Os parâmetros e configuração de uma instalação da linha de comando podem ser complementados pelo arquivo de configuração *.xml* do administrador, o "*cfg.xml*", que deve estar na mesma pasta do arquivo de instalação *msi* do ERA. O arquivo de configuração poderá ser criado no Editor de configuração da ESET e permite que você defina várias configurações do ERA. Consulte a seção Editor de configuração da ESET 50 para obter mais detalhes.

2.2.3.1.1 Instalação no modo de agrupamento

O cenário de **Instalação avançada** também permite que você ative a **Instalação no modo de agrupamento**. Se a Instalação no modo de agrupamento estiver habilitada, você precisará especificar o caminho para uma pasta de dados compartilhados de agrupamento que esteja totalmente acessível para todos os nós de agrupamento (ou seja, todos os nós devem ter permissões de leitura/gravação para essa pasta). Isso pode ser um disco de quorum ou uma pasta compartilhada de UNC. Se uma pasta compartilhada for usada, você deverá habilitar o compartilhamento para **Computadores** nas propriedades da pasta compartilhada. O nome do nó de cluster deverá então ser adicionado a **Compartilhar permissões** com direitos totais.

OBSERVAÇÃO: não recomendamos o uso de um endereço IP ao definir uma pasta compartilhada para o agrupamento.

É necessário instalar o ERA Server individualmente em todos os nós do agrupamento. Depois de cada instalação do ERA Server, a inicialização automática do Serviço ERA precisa ser alterada para manual. Quando o ERA Server for instalado em todos os nós, crie o serviço genérico (era_server). O serviço genérico deve ser dependente do recurso do nome da rede no administrador do agrupamento.

Se qualquer outro banco de dados que não seja o MS Access incorporado for usado, é importante se certificar de que todos os nós do ERA Server se conectam ao mesmo banco de dados. Nas próximas etapas, também é importante definir o nome do nó de agrupamento no qual o ERA será instalado como o nome do servidor.

Importante: é necessário configurar o serviço ESET Remote Administrator Server (ERA_SERVER) como o serviço genérico do agrupamento no console do administrador do agrupamento.

Desinstalação

Se você pretende desinstalar o ERA Server, o grupo de agrupamento deverá estar on-line para que o processo de desinstalação continue:

1) Cancele o agrupamento ao desativar um dos nós.

2) Deixe que o failover seja concluído para se certificar de que os outros nós estejam funcionando.

3) Desinstale o ESET Remote Administrator do nó desabilitado.

4) Reinicie o nó.

5) Vincule novamente o nó.

6) Repita as etapas acima para quaisquer nós adicionais no agrupamento.

Atualizando o ERA instalado no nó de agrupamento

Pela reinstalação do modo de agrupamento, é necessário que o grupo do serviço ERA de agrupamento fique off-line selecionando **Ficar off-line** no console do administrador do agrupamento. Em seguida, reinstale o ERA em todos os nós do agrupamento e coloque o grupo do serviço ERA do agrupamento on-line novamente.

2.2.3.2 Instalação do ERA Console

Instale o ESET Remote Administrator Console no PC/notebook do administrador. No final do modo de instalação avançada, insira o nome do ERA Server (ou seu endereço IP) ao qual o ERAC se conectará automaticamente na inicialização. Em nosso exemplo, ele é identificado como GHOST.

Depois da instalação, inicie o ERAC e verifique a conexão com o ERAS. Por padrão, não é necessário senha para se conectar a um ERA Server (o campo de texto da senha está em branco), mas recomendamos que uma seja estabelecida. Para criar uma senha para se conectar a um ERA Server, clique em **Arquivo** > **Alterar senha...** e então modifique a Senha para console clicando no botão **Alterar...**.

OBSERVAÇÃO: O administrador pode especificar uma conta de usuário e senha com acesso ao ESET Remote Administrator Console. O administrador também pode especificar o nível de acesso. Para obter mais informações, consulte o capítulo Gerenciador de usuários 94. O ERAC precisa ser instalado no computador, do qual você deseja acessar o ERAS com a conta definida no Gerenciador de usuários.

2.2.3.3 Imagem

Você pode usar o ERA Console para ativar o servidor de atualização de LAN - a imagem no ERA Server. Esse servidor poderá então ser usado para atualizar estações de trabalho localizadas na LAN. Ao ativar a imagem, você diminuirá o volume de dados transferidos através de sua conexão com a Internet.

Continue da seguinte forma:

1) Conecte o ERA Console ao ERA Server clicando em Arquivo > Conectar.

2) No ERA Console, clique em Ferramentas > Opções do servidor... e clique na guia Atualizações.

3) No menu suspenso Servidor de atualização, selecione Escolher automaticamente, deixe Intervalo de atualização em 60 minutos. Insira o nome do usuário de atualização (EAV-****) e clique em Definir senha... e digite ou cole a senha que você recebeu com seu nome de usuário.

4) Selecione a opção Criar imagem da atualização. Deixe o caminho padrão para arquivos da imagem e a porta do servidor HTTP (2221). Deixe a Autenticação como NONE.

5) Clique na guia Avançado e clique em Editar configurações avançadas... Na árvore de configuração avançada, acesse o ERA Server > Configuração > Imagem > Criar imagem dos componentes de programa selecionados. Clique em Editar no lado direito e selecione os componentes de programa a serem baixados. Componentes para todas as versões de idioma que serão usados na rede devem ser selecionados.

6) Na guia Atualizações, clique em Atualizar agora para criar a imagem.

Para obter opções de configuração de imagem mais detalhadas, consulte o capítulo Como ativar e configurar a Imagem 104.

2.2.3.4 Tipos de bancos de dados compatíveis com o ERA Server

Por padrão, o programa usa o mecanismo Microsoft Access (Jet Database). O ERAS 5.0 também é compatível com os seguintes bancos de dados:

- Microsoft SQL Server 2005 e versões posteriores
- MySQL 5.0 e versões posteriores
- Oracle 9i e versões posteriores

O tipo de banco de dados pode ser selecionado durante a instalação avançada do ERAS. Depois da instalação não é possível alterar o tipo de banco de dados diretamente do ERA; no entanto, você pode fazer isso usando a ERA Maintenance Tool 128.

OBSERVAÇÃO:

- O banco de dados Microsoft Access não é compatível com o Windows Server 2008 Core.
- O SQL Server Express tem um limite de tamanho de banco de dados de 4 GB.
- O banco de dados Microsoft Access tem um limite de tamanho de banco de dados de 2 GB.
- Ao usar o MySQL no Microsoft Windows 2000, recomendamos que você use driver ODBC 5.1.8 ou versão posterior para estabelecer uma conexão de banco de dados 18.

2.2.3.4.1 Requisitos básicos

Primeiro, é necessário criar o banco de dados em um servidor de banco de dados. O instalador do ERAS é capaz de criar um banco de dados vazio do MySQL, que é automaticamente nomeado ESETRADB.

Por padrão, o instalador cria automaticamente um novo banco de dados. Para criar o banco de dados manualmente, selecione a opção **Exportar script**. Certifique-se de que a opção **Criar tabelas automaticamente no novo banco de dados** esteja desmarcada.

Configurações de agrupamento

A classificação será realizada de acordo com as configurações padrão de cada banco de dados. É necessário ativar a CI (CASE INSENSIVITY, Não distinção entre letras maiúsculas e minúsculas).

Para ativar:

- Para MS SQL e MySQL, um comando COLLATE (Agrupamento) deve ser configurado com a CI ativada.
- Para ORACLE um NLS_SORT deve ser configurado com a CI ativada.
- Para MS Access nenhuma ação é necessária, pois a CI já está ativada.

Conjunto de caracteres

É importante usar o conjunto de caracteres UNICODE (recomenda-se UTF-8), especialmente quando os clientes têm locais específicos ou se o próprio ERA estiver operando em uma versão localizada. Se não houver plano para replicação e todos os clientes se conectarem ao mesmo servidor, você poderá usar o conjunto de caracteres para o local do ERA no qual você deseja instalar.

MARS (Multiple Active Result Sets, Vários conjuntos de resultados ativos)

Se um banco de dados MS SQL for usado, um driver ODBC com suporte para MARS será necessário para um perfeito funcionamento. Caso contrário, o servidor funcionará menos efetivamente e registrará a seguinte mensagem de erro no log do servidor:

Problema na conexão com o banco de dados. Recomenda-se usar um driver odbc que seja compatível com MARS (Multiple Active Result Sets, Vários conjuntos de resultados ativos). O servidor continuará em execução, mas a comunicação com o banco de dados poderá ficar mais lenta. Para obter mais informações, consulte a documentação ou entre em contato com o suporte da ESET.

Se o problema ocorrer com outro banco de dados que não seja o MS SQL, o servidor registrará a seguinte mensagem de erro no log do servidor e parará:

Problema na conexão com o banco de dados. Atualizar o driver odbc pode ajudar. Você também pode contatar o suporte da ESET para obter mais informações.

Drivers sem suporte para MARS:

- SQLSRV32.DLL (2000.85.1117.00)

- SQLSRV32.DLL (6.0.6001.18000) - originariamente contido no Windows Vista e Windows Server 2008

Driver original com suporte para MARS:

- SQLNCLI.DLL (2005.90.1399.00)

2.2.3.4.2 Configuração da conexão do banco de dados

Depois que um novo banco de dados for criado, você deverá especificar parâmetros de conexão para o servidor do banco de dados usando uma das duas opções:

1. Usando DSN (data source name, nome de origem de dados)
   Para abrir o DSN manualmente, abra o OBCD.
   Administrador da origem de dados
   (Clique em **Iniciar > Executar** - e insira *odbcad32.exe*).

   Exemplo de uma conexão de DSN:
   DSN =ERASqlServer

   Importante: o uso do *DSN do sistema* é recomendado para que o ERA funcione corretamente.

Importante: em um sistema operacional de 64 bits, o *odbcad32.exe* deverá ser executado da pasta *%SystemRoot%\SysWOW64*.

Para se certificar de que a instalação em MSSQL com autenticação do Windows/domínio foi bem-sucedida, certifique-se de usar o formato DNS ao inserir a cadeia de conexão.

2. Diretamente, usando uma cadeia de conexão completa
   Todos os parâmetros necessários devem ser especificados - driver, servidor e nome do banco de dados.

   Este é um exemplo de uma cadeia de conexão completa para MS SQL Server:
   Driver ={SQL Server}; Servidor =hostname; Banco de dados =ESETRADB

   Este é um exemplo de uma cadeia de conexão completa para Oracle Server:
   Driver ={Oracle em instantclient10_1}; dbq =hostname: 1521/ESETRADB

   Este é um exemplo de uma cadeia de conexão completa para MySQL Server:
   Driver ={MySQL ODBC 3.51 Driver}; Servidor =hostname; Banco de dados =ESETRADB

   Clique em **Definir** e especifique o **Nome de usuário** e **Senha** para sua conexão. As conexões de banco de dados Oracle e MS SQL Server também exigem um **Nome do esquema**.

   Clique em **Testar conexão** para verificar a conexão com o servidor do banco de dados.

OBSERVAÇÃO: recomendamos usar a autenticação do servidor de banco de dados em vez da autenticação do Windows/domínio.

2.2.3.5 Instalação em versões anteriores

O ESET Remote Administrator 5 é compatível com a instalação em versões anteriores, incluindo migração de dados. Para atualizar do ERA versão 1.x ou 2.x recomendamos que primeiro você migre os dados para uma instalação 4.x e depois instale a versão 5.x para preservar seus dados.

OBSERVAÇÃO: Recomendamos que você faça a reinstalação somente quando não houver clientes conectados, pois o ERA Server Service é interrompido e todas as conexões são encerradas durante o processo de reinstalação. A migração do banco de dados pode ser realizada antes ou após a reinstalação (consulte o capítulo Transferência do banco de dados 129 para obter mais informações).

- **Instalação do ERA Server**:

1. Faça download do arquivo de instalação no seu servidor. Para iniciar a instalação, dê um duplo clique no arquivo do instalador.

2. Selecione instalação Típica ou Avançada, semelhante a uma instalação limpa do ERA Server 14.

- **Instalação típica** - será solicitado seu arquivo de chave de licença (*.lic), senhas e dados de atualização. Há dois modos de migração: **Modo Importar somente configuração** cria tabelas vazias em um novo banco de dados; **Modo de importação completa**importa todos os dados do banco de dados. Selecionar **Criar backup de banco de dados atual** (padrão) criará um backup antes de fazer quaisquer alterações no banco de dados. **Ativar limpeza automática padrão para registros anteriores**pode ser selecionada para melhorar a manutenção do banco de dados.

- **Instalação avançada** - será solicitado seu arquivo de chave de licença (*.lic), a conta usada para executar o serviço ERA Server, portas usadas para comunicação, senhas e dados de atualização, configurações do Servidor SMTP (opcional), configurações de registro em log 96 e configurações de migração de banco de dados (descritas em **instalação Típica** acima). Durante a instalação avançada você terá a opção de migrar as políticas anteriores (Windows desktop v3 e v4) para as políticas novas (Windows desktop v5). A migração é realizada usando as configurações padrão, portanto se você quiser configurar a migração, recomendamos usar o Assistente de migração de política 73 depois da atualização ser concluída.

OBSERVAÇÃO: se o instalador encontrar quaisquer tabelas existentes no banco de dados atual, um aviso será exibido. Para substituir conteúdo de uma tabela existente, clique em **Substituir** (***Aviso:*** isso vai excluir o conteúdo de tabelas e substituir suas estruturas!). Clique em **Ignorar** para não modificar as tabelas. Clicar em **Ignorar** poderá causar erros de inconsistência no banco de dados, especialmente quando as tabelas estiverem danificadas ou incompatíveis com a versão atual.

Se você quiser analisar o banco de dados atual manualmente, clique em **Cancelar** para anular a instalação do ERAS.

- **Instalação do ERA Console**:

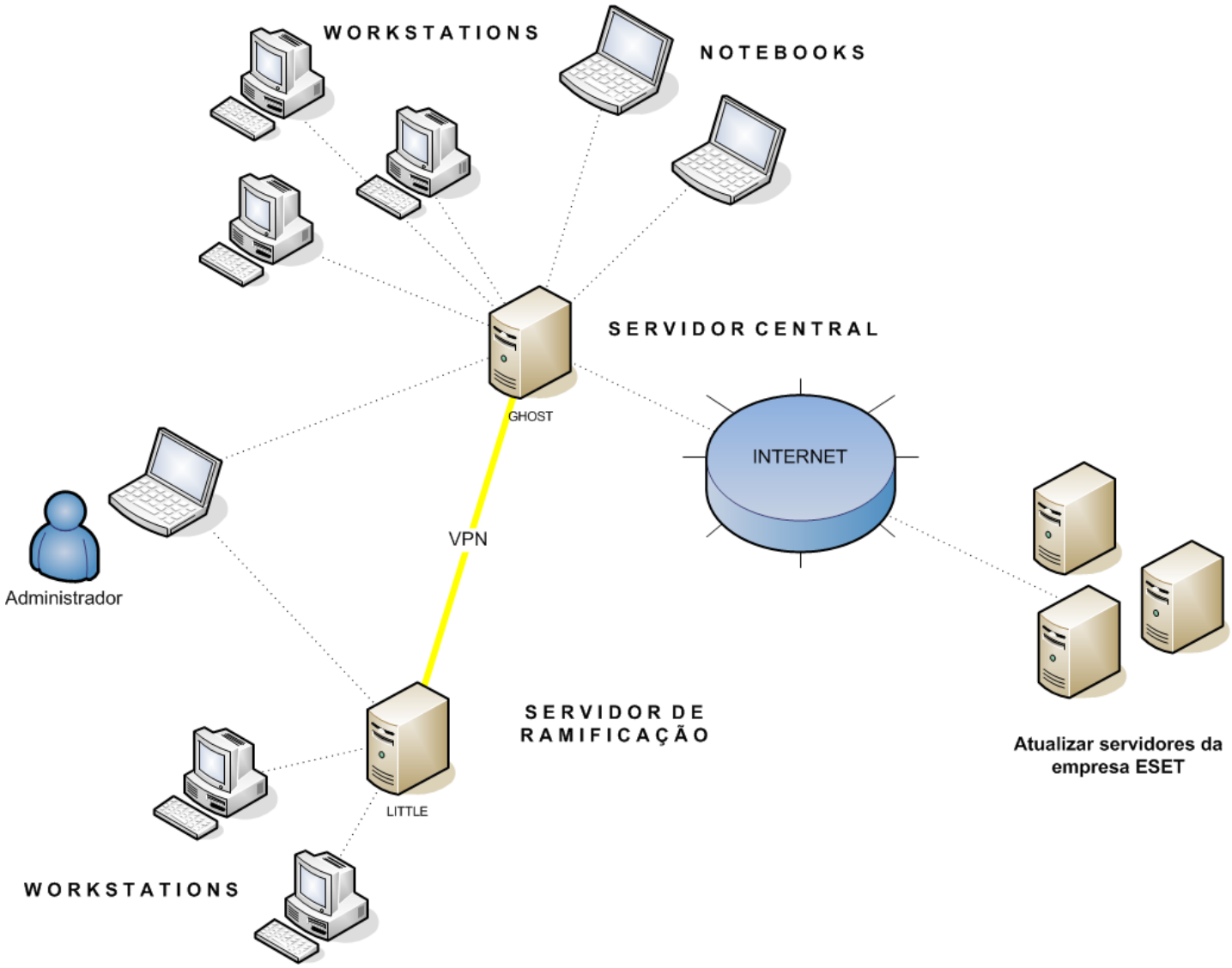
1. Faça download do arquivo de instalação no seu servidor. Para iniciar a instalação, dê um duplo clique no arquivo de instalação.

2. Proceda como descrito no capítulo Instalação do ERA Console 16.

2.3 Cenário - Instalação em um ambiente empresarial

2.3.1 Visão geral do ambiente (estrutura de rede)

A seguir é apresentada uma cópia da estrutura de rede anterior com uma filial adicional, vários clientes e um servidor nomeado LITTLE. Vamos supor que haja um canal VPN lento entre a sede e a filial. Nesse cenário, o servidor de imagem deve ser instalado no servidor LITTLE. Além disso, instalaremos um segundo ERA Server no LITTLE, a fim de criar um ambiente mais acessível e minimizar o volume de dados transferidos.

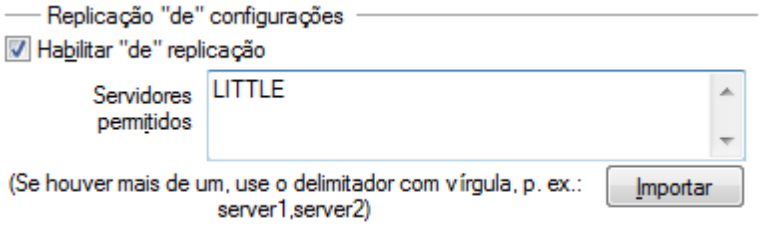


2.3.2 Instalação

2.3.2.1 Instalação em sede

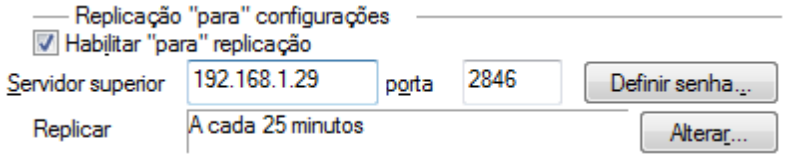
As instalações do ERAS, ERAC e estações de trabalho clientes são muito semelhantes ao cenário anterior. A única diferença está na configuração do ERAS principal (GHOST). Em **Ferramentas** > **Opções do servidor...** > **Replicação**, marque a caixa de seleção **Habilitar "de" replicação** e insira o nome do servidor secundário em **Servidores permitidos**. Em nosso caso, o servidor inferior é denominado LITTLE.

Se houver uma senha para a replicação definida no servidor superior (**Ferramentas** > **Opções do servidor...** > **Segurança** > **Senha para replicação**), então essa senha deverá ser usada para autenticação do servidor inferior.



2.3.2.2 Filial: Instalação do ERA Server

Como no exemplo diretamente acima, instale o segundo ERAS e ERAC. Novamente, ative e defina as configurações de replicação. Dessa vez, marque a caixa de seleção **Habilitar "para" replicação** (**Ferramentas** > **Opções do servidor...** > **Replicação**) e defina o nome do ERAS mestre. Recomendamos usar o endereço IP do servidor mestre, que é o endereço IP do GHOST do servidor.



2.3.2.3 Filial: Instalação do servidor de Imagem de HTTP

A configuração de instalação do servidor de imagem no cenário anterior também pode ser usada nesse caso. As únicas alterações são nas seções definindo o nome de usuário e senha.

Como na figura do capítulo Visão geral do ambiente 20, as atualizações para a filial não serão baixadas dos servidores de atualização da ESET, mas do servidor na sede (GHOST). A origem de atualização será definida pelo seguinte endereço de URL:

http://ghost:2221 (ou http://IP_address_of_ghost:2221)

Por padrão, não há necessidade de especificar um nome de usuário ou senha, pois o servidor HTTP integrado não requer autenticação.

Para obter mais informações sobre como configurar a imagem no ERAS, consulte o capítulo intitulado Servidor de imagem 102.

2.3.2.4 Filial: Instalação remota em clientes

Mais uma vez, o modelo anterior pode ser usado, exceto que é adequado para realizar todas as operações com o ERAC conectadas diretamente ao ERAS da filial (em nosso exemplo: LITTLE). Isso é feito para impedir que pacotes de instalação sejam transferidos através do canal VPN, que é mais lento.

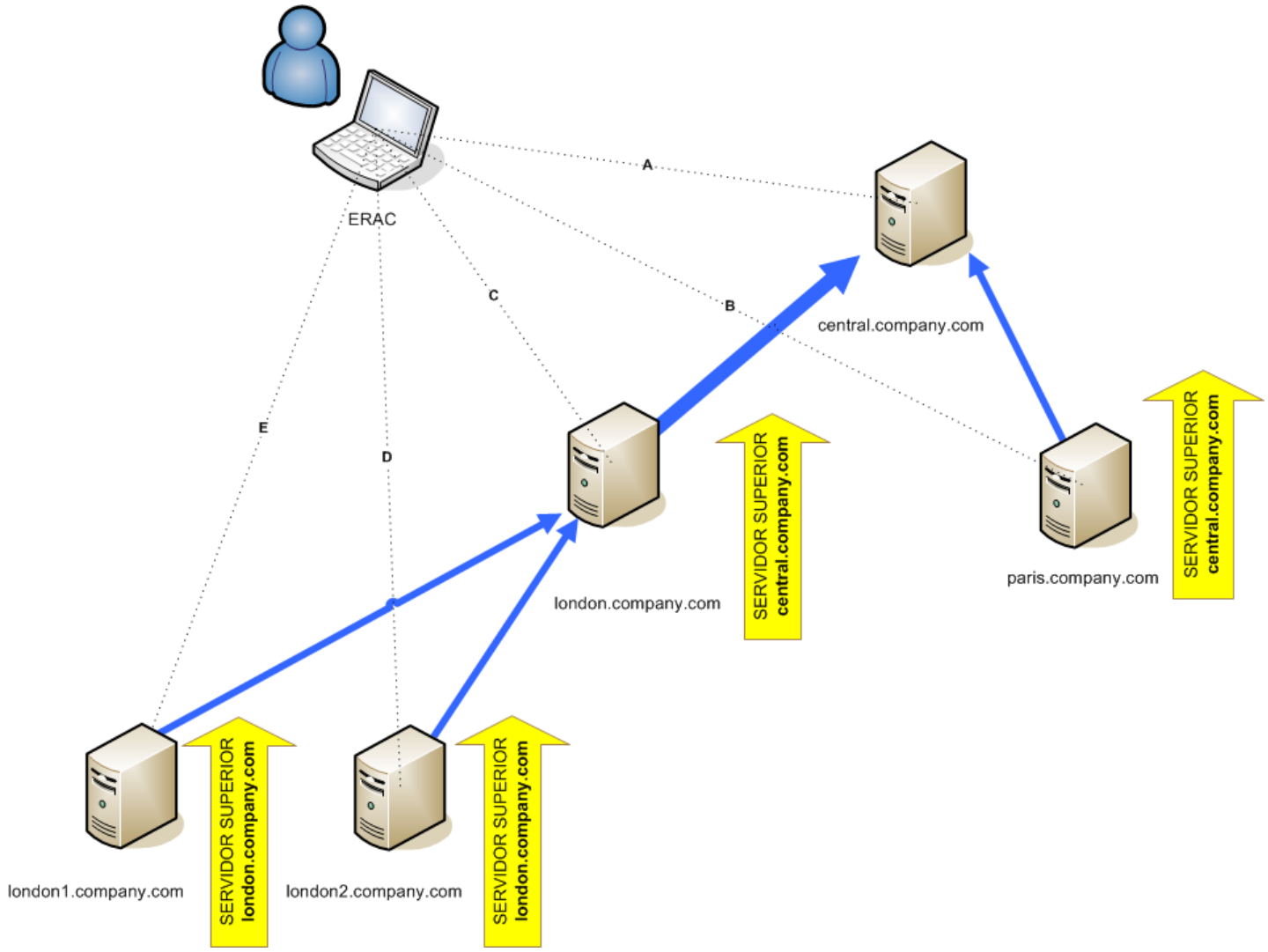
2.3.3 Outros requisitos para ambientes empresariais

Em redes maiores, vários ERA Servers podem ser instalados para realizar instalações remotas de computadores clientes de servidores que estão mais acessíveis. Para essa finalidade, o ERAS oferece *replicação* (consulte o capítulo Instalação em sede 21 e Filial: instalação do ERA Server 21), que permite que informações armazenadas sejam encaminhadas para um ERAS pai (*servidor superior*). A replicação pode ser configurada usando o ERAC.

O recurso de replicação é muito útil para empresas com várias filiais ou escritórios remotos. O cenário de implantação modelo seria o seguinte: instale o ERAS em cada escritório e faça uma replicata de cada em um ERAS central. A vantagem dessa configuração é especialmente aparente em redes privadas que estão conectadas via VPN, que é geralmente mais lenta - o administrador precisará apenas conectar-se a um ERAS central (a comunicação marcada pela letra A na figura a seguir). Não há necessidade de usar a VPN para acessar departamentos individuais (as comunicações B, C, D e E). O canal de comunicação mais lento é desviado através do uso de replicação do ERAS.

A configuração de replicação permite que um administrador defina quais informações serão transferidas automaticamente para servidores superiores em um intervalo predefinido, bem como quais informações serão enviadas mediante solicitação do administrador do servidor superior. A replicação torna o ERA mais acessível e também minimiza o tráfego de rede.

Outra vantagem de replicação é que vários usuários podem fazer login com vários níveis de permissão. O administrador acessando o ERAS london2.company.com com o console (comunicação D) pode controlar somente clientes conectando-se a london2.company.com. O administrador acessando o company.com (A) central pode controlar todos os clientes localizados na sede da empresa, bem como departamentos/filiais.



3. Trabalhar com o ERA Console

3.1 Conectando-se ao ERA Server

A maioria dos recursos no ERAC estão disponíveis somente após a conexão com o ERAS. Defina o servidor por nome ou endereço IP antes de se conectar:

Abra o ERAC e clique em **Arquivo** > **Editar conexões...** (ou **Ferramentas** > **Opções do console...**) e clique na guia **Conexão**.

Clique no botão **Adicionar/Remover...** para adicionar novos ERA Servers ou modificar servidores atualmente relacionados. Selecione o servidor desejado no menu suspenso **Selecionar conexão**. Em seguida, clique no botão **Conectar**.

OBSERVAÇÃO: o ERAC é totalmente compatível com o protocolo IPv6. O endereço deve estar no formato *[ipv6address]:porta*, por exemplo, *[::1]:2223*.

Outras opções nessa janela:

- **Conectar ao servidor selecionado na inicialização do console** - se esta opção for selecionada, o console se conectará automaticamente ao ERAS selecionado na inicialização.
- **Mostrar mensagem quando a conexão falhar** - se houver um erro de comunicação entre o ERAC e o ERAS, um alerta será exibido.

Há dois tipos de autenticação disponíveis:

ERA Server

O usuário fará a autenticação com as credenciais do ERAS. Por padrão, não é necessário senha para se conectar a um ERAS, mas recomendamos que uma seja estabelecida. Para criar uma senha para se conectar ao ERAS:

Clique em **Arquivo** > **Alterar senha...** (ou **Ferramentas** > **Opções do servidor** > **Segurança**) e então clique no botão **Alterar...** ao lado de **Senha para console**.

Ao inserir uma senha, você poderá marcar a opção **Lembrar senha**. Considere os possíveis riscos de segurança associados a essa opção. Para excluir todas as senhas lembradas, clique em **Arquivo** > **Limpar senhas armazenadas em cache...**.

Se você quiser definir ou alterar as contas de usuário para a autenticação Console-Servidor, use a ferramenta Gerenciador de usuários 94.

Windows/Domínio

Os usuários farão a autenticação com as credenciais de usuário do Windows/domínio. Para que a autenticação do Windows/domínio funcione corretamente, o ERAS precisará ser instalado na conta do Windows/domínio com direitos suficientes. Você também deve habilitar esse recurso na guia **Ferramentas** > **Opções do servidor...** > **Avançadas** > **Editar configurações avançadas...** > **ESET Remote Administrator** > **ERA Server** > **Configuração** > **Segurança**:

Permitir autenticação do Windows/domínio - habilita/desabilita a autenticação do Windows/domínio.

Grupos do administrador - permite que você defina grupos para os quais a autenticação do Windows/domínio será habilitada.

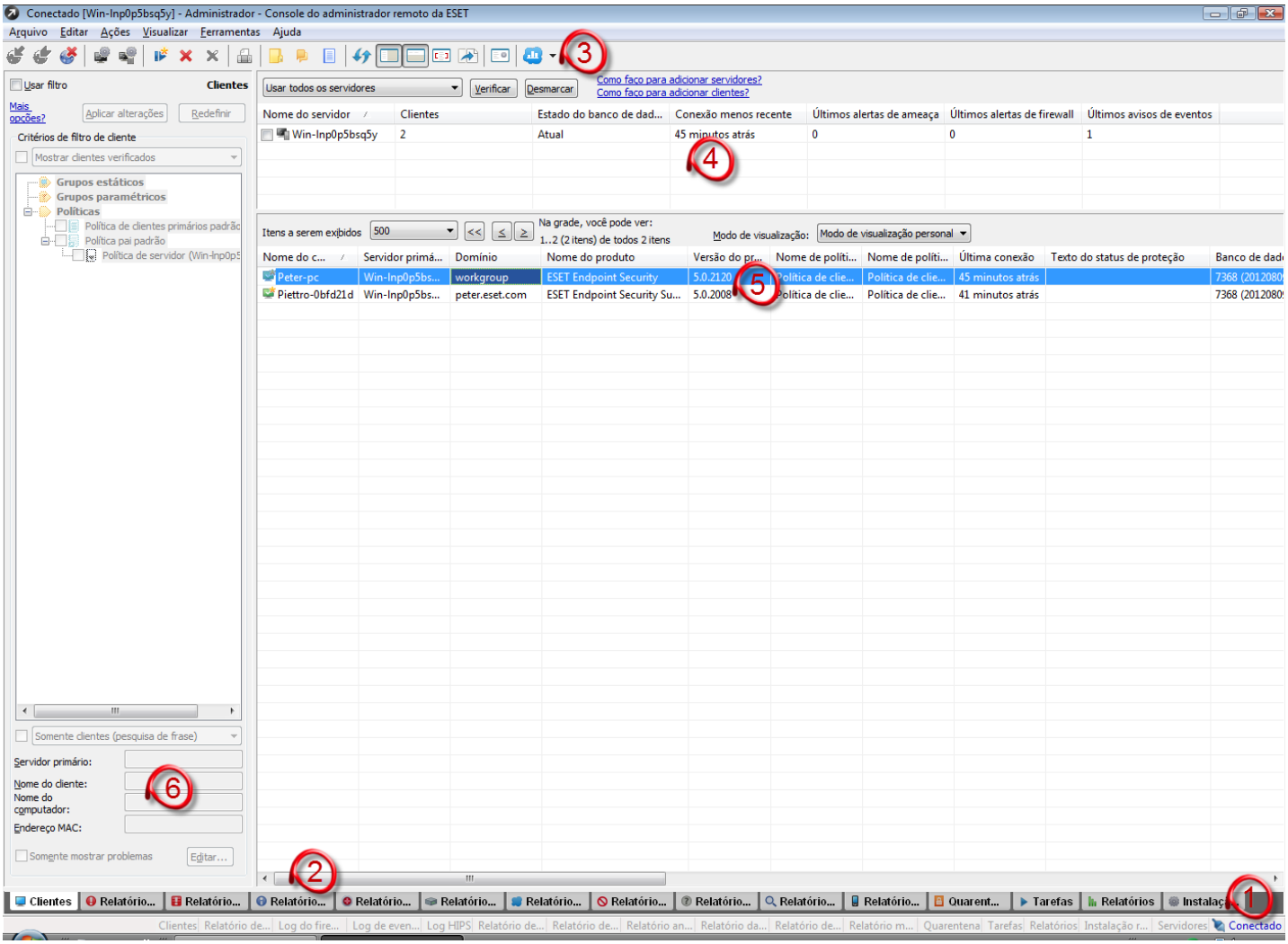
Grupos somente leitura - permite que você defina grupos com acesso somente leitura.

Quando a comunicação tiver sido estabelecida, o cabeçalho do programa será alterado para **[server_name] conectado** .

Como alternativa, você pode clicar em **Arquivo** > **Conectar** para se conectar ao ERAS.

OBSERVAÇÃO: a comunicação entre o ERAC e o ERAS é criptografada (AES-256).

3.2 ERA Console - janela principal



O status de comunicação atual entre o ERAC e o ERAS será exibido na barra de status (**1**). Todos os dados necessários do ERAS serão atualizados regularmente (o padrão é a cada minuto. Consulte **Ferramentas** > **Opções do console** > **Outras configurações** > **Usar atualização automática (m)**. O progresso de atualização também poderá ser visto na barra de status.

OBSERVAÇÃO: Pressione F5 para atualizar dados exibidos.

As informações serão divididas em várias guias 28 na ordem de importância (**2**). A maioria das informações em guias está relacionada aos clientes conectados. Na maioria dos casos, os dados podem ser classificados em ordem ascendente ou descendente clicando em um atributo (**5**), enquanto uma operação de arrastar e soltar pode ser usada para reorganização. Se várias linhas de dados forem ser processadas, você poderá limitá-las usando o menu suspenso **Itens a serem exibidos** e os botões **procurar página por página**. Selecione o **Modo de visualização** para exibir atributos de acordo com a sua necessidade (para obter mais detalhes, consulte o capítulo Filtragem de informações 25. Se você precisar imprimir determinadas informações das guias, consulte o capítulo Configuração de página 25 para obter mais informações.

A seção do Servidor (**4**) é importante se você replicar ERA Servers. Essa seção exibe informações de resumo sobre o Console ao qual o ERAS está conectado, bem como informações sobre ERA Servers filhos ou "inferiores". O menu suspenso Servidores na seção **4** influenciará o escopo de informações exibidas na seção **5**.

- **Usar todos os servidores -** exibe informações de todos os ERA Servers - seção (**5**).
- **Usar somente servidores selecionados -** exibe informações dos ERA Servers selecionados - seção (**5**).
- **Excluir servidores selecionados -** exibe informações dos ERA Servers selecionados.

Colunas na Seção **4**:

- **Nome do servidor** - exibe o nome do servidor.

- **Clientes** - número total de clientes conectando-se ou no banco de dados do ERAS selecionado.
- **Intervalo de banco de dados de assinatura de vírus** - versão de bancos de dados de assinatura de vírus entre os clientes do ERAS selecionado.
- **Conexão menos recente** - tempo decorrido desde a conexão menos recente ao servidor.
- **Últimos alertas de ameaça** - o número total de alertas de vírus (consulte o atributo **Último alerta de ameaça** na seção **5**).
- **Últimos alertas de firewall** - o número total de alertas de firewall.
- **Últimos avisos de evento** - o número total de eventos atuais (consulte o atributo **Último evento** na seção **5**).

Se não estiver conectado no momento, você poderá clicar com o botão direito do mouse na seção do Servidor (**4**) e selecione **Conectar a este servidor** para conectar-se ao ERAS escolhido. Mais informações serão exibidas na seção do Servidor (**4**) se a replicação estiver habilitada.

Os recursos mais importantes do ERAC estão acessíveis no menu principal ou na barra de ferramentas do ERAC (**3**).

A última seção é **Critérios do filtro de computador** (**6**) - consulte o capítulo intitulado Filtragem de informações 25.

OBSERVAÇÃO: Recomendamos usar o menu Contexto 27 para administrar informações de filtro e clientes. Essa é uma forma rápida para executar tarefas, gerenciar grupos e políticas, filtrar dados e muito mais.

3.2.1 Configuração de página

Na janela **Configuração de página**, você pode definir parâmetros para impressão do conteúdo de guias no ERA Console:

WYSIWYG - imprime guias exatamente como você as vê (What You See Is What You Get, O que você vê é o que você obtém).

Imprimir - imprime guias em escala de cinzas. Somente as cores preto e branca são usadas.

Ícone de impressão - imprime também ícones exibidos ao lado de nomes de clientes.

Cabeçalho de impressão - insere a cadeia de caracteres definida em **Cabeçalho** no canto esquerdo superior. Use o cabeçalho padrão ou escreva seu próprio cabeçalho no campo **Cabeçalho**.

Logotipo de impressão - insere a cadeia de caracteres definida em **Caminho do logotipo** no canto direito superior. Por padrão, será impresso o logotipo da ESET. Você pode carregar seu próprio logotipo clicando no botão **"..."** ao lado dessa opção e escolhendo o logotipo de sua unidade de disco rígido.

Numerar páginas - insere o número de página na seção inferior da página impressa.

Visualizar - clique para exibir uma visualização da página impressa.

3.3 Filtragem de informações

O ERAC oferece várias ferramentas e recursos que fornecem administração acessível de clientes e eventos. Ter um sistema avançado de filtragem frequentemente é essencial, especialmente em sistemas com um grande número de clientes, quando as informações exibidas precisam ser agrupadas e facilmente gerenciáveis. Há várias ferramentas no ERAC que permitem que você classifique e filtre com eficiência informações sobre os clientes conectados.

O Filtro 26 permite que os administradores visualizem somente informações relacionadas a estações de trabalho clientes ou servidores específicos. Para mostrar as opções de filtro, clique em **Visualizar** > **Mostrar/Ocultar painel de filtro** no menu ERAC.

Modo de visualização

O número de colunas exibidas na guia **Clientes** pode ser ajustado usando o menu suspenso **Modo de visualização** no lado direito do Console. O **Modo de visualização completa** exibe todas as colunas, enquanto o **Modo de visualização mínima** mostra somente as colunas mais importantes. Esses módulos são predefinidos e não podem ser modificados. Para personalizar sua visualização, selecione **Modo de visualização personalizada**. Ela pode ser configurada na guia **Ferramentas** > **Opções do console...** > **Colunas** > **Mostrar/Ocultar**.

3.3.1 Filtro

Para ativar a filtragem, selecione **Usar filtro** no lado esquerdo superior do ERAC. Quaisquer futuras modificações nos critérios de filtro atualizarão automaticamente dados exibidos, exceto os configurados de outra forma em **Ferramentas** > **Opções do console...** > **Outras configurações**.

Defina os critérios de filtragem na seção **Critérios de filtro de cliente**. Os clientes podem pertencer a vários grupos e políticas. Atribuir um cliente a um grupo estático ou paramétrico poderá se comprovar muito útil, não somente para fins de filtragem, mas também para atividades como geração de relatórios. Para saber mais sobre o gerenciamento de grupos, consulte o capítulo intitulado Gerenciador de grupos 69. O uso de políticas para segregação de clientes também pode atender a várias funções. Para obter mais informações sobre a criação e o gerenciamento de políticas, consulte o capítulo Políticas 71.

A primeira ferramenta de filtragem será a seção de seleção de grupo e política. Há três opções disponíveis:

- **Mostrar clientes verificados** - os clientes em grupos/políticas selecionados serão exibidos no painel **Clientes**.
- **Ocultar clientes verificados** - os clientes em grupos/políticas que não forem selecionados e clientes em nenhum grupo serão exibidos no painel **Clientes**. Se um cliente for um membro de vários grupos e um dos grupos for verificado, o cliente não será exibido.
- **Ocultar clientes verificados, ignorar associação múltipla** - os clientes em grupos/políticas que não forem selecionados e clientes em nenhum grupo serão exibidos. Se um cliente for um membro de mais grupos e um dos grupos for verificado, o cliente será exibido.
- **Mostrar clientes em nenhum grupo** - somente clientes que não pertencerem a qualquer grupo/política serão exibidos.

OBSERVAÇÃO: ao verificar um grupo da lista, todos os seus subgrupos também serão verificados.

Na parte inferior da seção **Filtro**, você poderá especificar outro conjunto de parâmetros:

- **Somente clientes (usando palavras inteiras)** - a saída inclui clientes com nomes idênticos à cadeia inserida.
- **Somente clientes iniciando como (?,*)** - a saída relacionará somente clientes com nomes iniciando com a cadeia especificada.
- **Somente clientes como (?,*)** - a saída relacionará somente clientes com nomes contendo a cadeia especificada.
- **Excluir clientes (usando palavras inteiras), Excluir clientes iniciando como (?,*), Excluir clientes como (?,*)** - estas opções gerarão resultados opostos à árvore anterior.

Os campos **Servidor primário**, **Nome do cliente**, **Nome do computador** e **Endereço MAC** aceitam cadeias com base nos critérios definidos no menu suspenso acima. Se qualquer um desses for preenchido, uma consulta de banco de dados será executada e os resultados serão filtrados com base no campo preenchido (o operador lógico AND (E) poderá ser usado). Você pode usar cadeias inteiras ou caracteres curinga (?,*).

A última opção é a filtragem com base em problemas - as saídas incluirão somente clientes com o tipo de problema especificado. Para exibir uma seleção de problemas, selecione **Somente mostrar problemas** e clique **Editar...**. Selecione os problemas que deseja que sejam exibidos e clique em **OK** para mostrar uma lista de clientes com os problemas selecionados.

Todas as alterações feitas na configuração de filtragem serão aplicadas depois de clicar em **Aplicar alterações**. Para restaurar padrões, clique em **Redefinir**. Para gerar automaticamente novas saídas depois de cada modificação das configurações de filtragem, clique em **Ferramentas** > **Opções do console...** > **Outras configurações...** e selecione **Aplicar alterações automaticamente**.

OBSERVAÇÃO: os critérios de filtro na última seção podem variar dependendo da guia atualmente ativa. Os critérios serão personalizados para classificar com eficácia os logs. Por exemplo, você pode classificar os logs pelo nível de detalhamento no log de firewall, a fim de exibir somente o tipo de logs que você precisa revisar.

Você também pode classificar os dados nas guias selecionando o intervalo de tempo para o qual deseja que os itens sejam exibidos. Para obter mais informações sobre como usar o **Filtro de data**, consulte o capítulo Filtro de data 27.

3.3.2 Menu de contexto

Use o botão direito do mouse para chamar o menu de contexto e ajuste a saída em colunas. Entre as opções do menu de contexto estão:

- **Selecionar tudo** - seleciona todas as entradas.
- **Selecionar por '...'** - esta opção permite que você clique com o botão direito do mouse em qualquer atributo, bem como selecione (realce) automaticamente todas as outras estações de trabalho ou servidores com o mesmo atributo. A cadeia ... será automaticamente substituída pelo valor da guia atual.
- **Seleção inversa** - realiza a seleção invertida de entradas.
- **Ocultar selecionados** - oculta entradas selecionadas.
- **Ocultar não selecionados** - oculta todas as entradas não selecionadas na lista.

OBSERVAÇÃO: as opções podem variar dependendo da janela atualmente ativa.

- **Mostrar/ocultar colunas** - abre a janela **Opções do console** > Colunas - Mostrar/ocultar 48 na qual você pode definir colunas que estarão disponíveis no painel selecionado.

As opções **Ocultar selecionados/não selecionados** são eficazes se for necessário mais organização depois de usar métodos de filtragem anteriores. Para desabilitar todos os filtros definidos pelo menu de contexto, clique em **Exibir** > **Exibição recortada** ou clique no ícone na barra de ferramentas do ERAC. Você também pode pressionar **F5** para atualizar informações exibidas e desabilitar filtros.

Exemplo:

- Para exibir somente clientes com alertas de ameaça:
  Na guia **Clientes**, clique com o botão direito do mouse em qualquer painel vazio com Último alerta de vírus e escolha **Selecionar por '...'** no menu de contexto. Então, novamente no menu de contexto, clique em **Ocultar selecionados**.
- Para exibir alertas de ameaça para os clientes "Joseph" e "Charles":
  Clique na guia **Log de ameaça** e clique com o botão direito do mouse em qualquer atributo na coluna Nome do cliente com o valor Joseph. No menu de contexto, clique em **Selecionar por 'Joseph'**. Em seguida, pressione e mantenha pressionada a tecla CTRL, clique com o botão direito do mouse e clique em **Selecionar por 'Charles'**. Por fim, clique com o botão direito do mouse e selecione **Ocultar não selecionados** no menu de texto e solte a tecla CTRL.

A tecla CTRL pode ser usada para selecionar/desselecionar entradas específicas; a tecla SHIFT poderá ser usada para marcar/desmarcar um grupo de entradas.

OBSERVAÇÃO: a filtragem também pode ser usada para facilitar a criação de novas tarefas para clientes específicos (selecionados). Há muitas formas de usar a filtragem com eficácia; tente com várias combinações.

3.3.3 Filtro de data

O **Filtro de data** está localizado no canto inferior direito de cada guia no ERAC. Ao especificar o **Intervalo DateTime**, você pode classificar facilmente dados de um período de tempo selecionado.

Últimas X horas/dias/semanas/meses/anos - selecione o número e hora especificados. Isso limitará os itens na guia atual e somente os itens desse intervalo de tempo serão exibidos. Por exemplo, se você selecionar *Últimos 10 dias*, todos os itens dos últimos 10 dias serão exibidos.

Últimos X - no menu suspenso, selecione o intervalo de tempo predefinido para o qual você deseja que os itens sejam mostrados.

Tudo antes (inclusive)/Tudo após (inclusive) - marque a caixa de seleção ao lado de **Tudo antes (inclusive)** ou **Tudo após (inclusive)** e especifique uma hora e data. Todos os itens antes/após essa hora e data serão exibidos.

Tudo no intervalo - selecione uma hora e data de início e fim. Os itens desse intervalo de tempo serão mostrados.

OBSERVAÇÃO: você pode usar um **Filtro de data** em cada log para especificar o intervalo de tempo para o qual você deseja que os dados sejam exibidos na guia. Você também tem a opção de definir o nível de detalhamento nas guias (onde aplicável) para classificar os dados por relevância. O **Filtro de data** exibirá os dados que já estão filtrados pelo filtro **Itens a serem exibidos** - esses filtros são dependentes. Isso significa que ele aplicará o filtro somente em dados já filtrados.

3.4 Guias no ERA Console

3.4.1 Descrição geral de guias e clientes

A maioria das informações em guias está relacionada aos clientes conectados. Cada cliente conectado ao ERAS é identificado pelos seguintes atributos:

Nome do computador (nome do cliente) + endereço MAC + servidor primário

O comportamento do ERAS em relação a determinadas operações de rede (como renomear um PC) pode ser definido na Configuração avançada do ERAS. Isso pode ajudar a impedir entradas duplicadas na guia **Clientes**. Por exemplo, se um dos computadores na rede tiver sido renomeado, mas seu endereço MAC permanecer inalterado, uma nova entrada não será criada na guia **Clientes**.

Clientes que se conectam ao ERAS pela primeira vez são designados por um valor **Sim** na coluna **Novo cliente**. Eles também são marcados por um asterisco pequeno no canto superior direito do ícone do cliente (veja a figura a seguir). Esse recurso permite que um administrador detecte facilmente um computador recentemente conectado. Esse atributo pode ter diferentes significados dependendo dos procedimentos operacionais do administrador.

Se um cliente tiver sido configurado e movido para um determinado grupo, o status Novo poderá ser desabilitado clicando-se com o botão direito do mouse no cliente e selecionando **Definir/redefinir sinalizadores** > **Redefinir sinalizador "Novo"**. O ícone do cliente alterará para o mostrado na figura a seguir e o valor na coluna **Novo cliente** será alternado para **Não**.

OBSERVAÇÃO: o atributo Comentário é opcional em todas as três guias. O administrador pode inserir qualquer descrição aqui (p. ex., *"Escritório número 129"*).

Os valores de tempo no ERAS podem ser exibidos no modo relativo (*"2 dias atrás"*), no modo absoluto (20.5.2009) ou no modo de sistema (configurações regionais).

Na maioria dos casos, os dados podem ser classificados em ordem ascendente ou descendente clicando em um atributo, enquanto uma operação de arrastar e soltar pode ser usada para reorganização.

Use a opção **Itens a serem exibidos** para classificar dados que você deseja exibir em uma guia. Defina o número de logs que você deseja exibir (o padrão é 200 para todos os logs) e o período de tempo a partir do qual você deseja que os logs sejam exibidos (por padrão, a partir dos últimos 7 dias). Em redes maiores, recomenda-se definir o período de tempo como **Não limitar o tempo**, pois isso pode causar uma intensa carga no banco de dados - e possivelmente diminuir o desempenho.

OBSERVAÇÃO: você pode usar um **Filtro de data** em cada log para especificar o intervalo de tempo para o qual você deseja que os dados sejam exibidos na guia. Você também tem a opção de definir o nível de detalhamento nas guias (onde aplicável) para classificar os dados por relevância. O **Filtro de data** exibirá os dados que já estão filtrados pelo filtro **Itens a serem exibidos** - esses filtros são dependentes.

Dar um duplo clique em determinados valores ativará outras guias e exibirá informações mais detalhadas. Por exemplo, se você dar um duplo clique em um valor na coluna **Último alerta de ameaça**, o programa passará para a guia **Log de ameaça** e exibirá entradas do log de ameaça relacionadas a determinado cliente. Se você der um duplo clique em um valor que contém muitas informações a serem exibidas em um modo de exibição com guias, uma janela da caixa de diálogo será aberta, mostrando informações detalhadas sobre o cliente correspondente.

3.4.2 Replicação e informações em guias individuais

Se o ERAC estiver conectado a um ERAS que esteja operando como um servidor superior, os clientes dos servidores inferiores serão exibidos automaticamente. Os tipos de informações replicadas podem ser configurados no servidor inferior em **Ferramentas** > **Opções do servidor** > **Replicação** > **Configurações de replicar "para"**.

Nesse cenário, as seguintes informações podem estar faltando:

- Logs de alerta detalhados (guia **Log de ameaça**)
- Logs de scanner sob demanda detalhados (guia **Log de rastreamento**)
- Configurações detalhadas do cliente atual no formato .xml (a guia **Clientes**, a coluna **Configuração**, **Status de proteção**, **Recursos de proteção**, **Informações sobre o sistema**)

As informações do programa ESET SysInspector também podem estar faltando. O ESET SysInspector está integrado aos produtos da ESET de geração 4.x e posteriores.

Se as informações não puderem ser encontradas nas janelas da caixa de diálogo do programa, clique no botão **Solicitar** (disponível em **Ações** > **Propriedades** > **Configuração**). Clicar nesse botão fará download das informações faltando de um ERAS inferior. Como a replicação é sempre iniciada por um ERAS inferior, as informações faltando serão entregues no intervalo de replicação predefinido.

No servidor superior, você poderá definir o nível de logs que serão recebidos pelo servidor (**Ferramentas** > **Opções do servidor** > **Avançado** > **Editar configurações avançadas...** > **ESET Remote Administrator** > **ERA Server** > **Configuração** > **Manutenção do servidor** > **.... logs para aceitar**).

OBSERVAÇÃO: essa opção se aplica a todos os clientes conectados ao servidor (não somente os replicados).

3.4.3 Guia Clientes

Esta guia exibe informações gerais sobre clientes individuais.

Atributo	Descrição
Nome do cliente	Nome do cliente (pode ser alterado na caixa de diálogo de propriedades do cliente - guia Geral)
Nome do computador	Nome da estação de trabalho/servidor (nome de host)
Endereço MAC	Endereço MAC (adaptador de rede)
Servidor primário	Nome do ERAS com o qual um cliente está se comunicando
Domínio	Nome do domínio/grupo ao qual um cliente pertence (esses não são grupos criados no ERAS)
IP	Endereço IPv4 ou IPv6
Nome do produto	Nome do produto da ESET
Versão do produto	Versão do produto da ESET
Nome da política	Nome de política atribuída a um cliente
Última conexão	Hora em que o cliente se conectou pela última vez ao ERAS (todos os outros dados coletados de clientes incluem esse registro, exceto para alguns dados obtidos pela replicação)
Texto do status de proteção	Status atual do produto de segurança da ESET instalado em um cliente
BD de assinatura de vírus	Versão do banco de dados de assinatura de vírus
Último alerta de ameaça	Último incidente de vírus
Último alerta de firewall	Último evento detectado pelo ESET Smart Security Personal Firewall (eventos do nível de aviso e superiores são mostrados)
Último aviso de evento	Última mensagem de erro
Últimos arquivos rastreados	Número de arquivos rastreados durante o último rastreamento sob demanda
Últimos arquivos infectados	Número de arquivos infectados encontrados durante o último rastreamento sob demanda
Últimos arquivos limpos	Número de arquivos limpos (ou excluídos) durante o último rastreamento sob demanda
Data do último rastreamento	Data do último rastreamento sob demanda
Solicitação de reinício	Requer uma reinicialização (p. ex., após a atualização de um programa)

Atributo	Descrição
Data da solicitação de reinício	Hora da primeira solicitação de reinício
Último produto iniciado	Hora em que o programa cliente foi iniciado pela última vez
Data de instalação do produto	Data em que o produto de segurança da ESET foi instalado no cliente
Usuário em roaming	Clientes com este atributo realizarão a tarefa "atualizar agora" sempre que estabelecerem uma conexão com o ERAS (recomendado para notebooks). A atualização será realizada somente se o banco de dados de assinatura de vírus do cliente não for atualizado. Esse recurso é útil para usuários que não tenham sido conectados ao ERAS por um longo período e esta tarefa causa a atualização imediata (mesmo antes da tarefa de atualização regular).
Novo cliente	Computador recentemente conectado (consulte o capítulo Descrição geral de guias e clientes 28)
Nome do SO	Nome do sistema operacional do cliente
Plataforma de SO	Plataforma de sistema operacional (Windows/Linux...)
Plataforma de HW	32 bits/64 bits
Configuração	Configuração .xml atual do cliente (incluindo data/hora em que a configuração foi criada)
Status de proteção	Declaração de status geral (semelhante em natureza ao atributo de configuração)
Recursos de proteção	Declaração de status geral para componentes do programa (semelhante ao atributo de configuração)
Informações sobre o sistema	O cliente envia informações do sistema para o ERAS (incluindo a hora em que as informações do sistema foram enviadas)
SysInspector	Clientes com a ferramenta ESET SysInspector instalada poderão enviar logs desse aplicativo.
Informações personalizadas 1, 2, 3	As informações personalizadas a serem exibidas especificadas pelo administrador (essa opção pode ser configurada no ERAC na guia Ferramentas > Opções do servidor... > Avançadas > Editar configurações avançadas... > ESET Remote Administrator > ERA Server > Configuração > Outras configurações > Informações personalizadas do cliente 1, 2, 3).
Comentário	Um breve comentário descrevendo o cliente (inserido pelo administrador)

OBSERVAÇÃO: alguns desses valores destinam-se somente para fins informativos, e podem não estar atualizados no momento em que o administrador os visualizar no Console. Por exemplo, informações sobre um erro de atualização que ocorreu às 7h não necessariamente significam que a atualização não foi concluída com êxito às 8h. O **Último alerta de ameaça** e **Último aviso de evento** podem ser considerados entre esses valores. Se o administrador souber que informações específicas estão obsoletas, elas poderão ser apagadas clicando-se com o botão direito do mouse e selecionando-se **Limpar informações** > **Limpar informações de "Último alerta de ameaça"** ou **Limpar informações do "Último aviso de evento"**. Informações sobre o último incidente de vírus ou o último evento do sistema serão excluídas.

Dar um duplo clique em um cliente exibirá opções adicionais na guia **Cliente**:

- **Geral** - contém informações semelhantes às que são exibidas na guia Clientes. Você pode usar essa guia para alterar o Nome do cliente - o nome com o qual um cliente estará visível no ERA e adicionar um comentário opcional.
- **Membro de grupos** - esta guia relaciona todos os grupos aos quais o cliente pertence. Para obter mais informações, consulte Filtragem de informações 25.
- **Tarefas** - exibe tarefas relacionadas ao cliente especificado. (para obter mais informações, consulte o capítulo Tarefas 64.
- **Configuração** - esta guia permite que você veja ou exporte a configuração do cliente atual para um arquivo .xml. Posteriormente neste manual, explicaremos como os arquivos *.xml* podem ser usados para criar um modelo de configuração para arquivos de configuração *.xml* novos/modificados. Para obter mais informações, consulte Tarefas 64.
- **Status de proteção** - esta é uma visão geral do status geral de todos os programas da ESET. Algumas das declarações são interativas e permitem intervenção imediata. Essa funcionalidade é útil, pois elimina a necessidade de definir manualmente uma nova tarefa para resolução de problemas específicos de proteção.
- **Recursos de proteção** - status de componente de todos os recursos de segurança da ESET (Antispam, Personal Firewall, etc.)
- **Informações do sistema** - informações detalhadas sobre o programa instalado, sua versão de componente do programa, etc.
- **SysInspector** - informações detalhadas sobre processos de inicialização e processos executados no segundo plano.
- **Quarentena** - contém uma lista de arquivos em quarentena. Os arquivos em quarentena podem ser solicitados de um cliente e salvos em um disco local.

Para realizar ações de rede para clientes específicos, clique com o botão direito em um cliente (ou clientes) e selecione **Ação da rede** do menu de contexto. Você terá várias opções - **Ping**, **Wake On LAN**, **Compartilhar**, **Desligar/Reiniciar**, **Mensagem**, **RDP** ou **Personalizado...**. Essas ações de rede correspondem às ações de rede do Windows com a mesma função. Cada ação de rede realizada (exceto Ping) informará a você sobre o estado da ação através da barra de progresso na janela de diálogo.

3.4.4 Guia Log de ameaças

Esta guia contém informações detalhadas sobre incidentes de ameaças ou vírus individuais.

Atributo	Descrição
Nome do cliente	Nome do cliente reportando o alerta de ameaça
Nome do computador	Nome da estação de trabalho/nome do servidor (nome de host)
Endereço MAC	Endereço MAC (adaptador de rede)
Servidor primário	Nome do ERAS com o qual um cliente está se comunicando
Data de recebimento	Horário no qual o evento foi registrado pelo ERAS
Data de ocorrência	Horário no qual o evento ocorreu
Nível	Nível de alerta
Scanner	Nome do recurso de segurança que detectou a ameaça
Objeto	Tipo de objeto
Nome	Geralmente, uma pasta na qual a infiltração está localizada
Ameaça	Nome do código malicioso detectado
Ação	Ação realizada pelo recurso de segurança específico
Usuário	Nome do usuário que foi identificado quando o incidente ocorreu
Informações	Informações sobre a ameaça detectada
Detalhes	Status de envio do log do cliente

3.4.5 Guia Log do firewall

Esta guia exibe informações relacionadas à atividade de firewall do cliente.

Atributo	Descrição
Nome do cliente	Nome do cliente reportando o evento
Nome do computador	Nome da estação de trabalho/nome do servidor (nome de host)
Endereço MAC	Endereço MAC (adaptador de rede)
Servidor primário	Nome do ERAS com o qual um cliente está se comunicando
Data de recebimento	Horário no qual o evento foi registrado pelo ERAS
Data de ocorrência	Horário no qual o evento ocorreu
Nível	Nível de alerta
Evento	Descrição do evento
Origem	Endereço IP de origem
Destino	Endereço IP de destino
Protocolo	Protocolo em questão
Regra	Regra de firewall em questão
Aplicativo	Aplicativo em questão
Usuário	Nome do usuário que foi identificado quando o incidente ocorreu

3.4.6 Guia Log de eventos

Esta guia mostra uma lista de todos os eventos relacionados ao sistema (com base nos componentes do programa de produto de segurança da ESET).

Atributo	Descrição
Nome do cliente	Nome do cliente reportando o evento
Nome do computador	Nome da estação de trabalho/servidor (nome de host)
Endereço MAC	Endereço MAC (adaptador de rede)
Servidor primário	Nome do ERAS com o qual um cliente está se comunicando
Data de recebimento	Horário no qual o evento foi registrado pelo ERAS
Data de ocorrência	Horário no qual o evento ocorreu
Nível	Nível de alerta
Plug-in	Nome do componente do programa reportando o evento
Evento	Descrição do evento
Usuário	Nome do usuário associado ao evento

3.4.7 Guia Log do HIPS

Esta guia mostra toda a atividade relacionada ao HIPS.

Atributo	Descrição
Id de HIPS	ID da entrada correspondente no banco de dados (a ID tem a forma: Número do HIPS)
Nome do cliente	Nome do cliente reportando a mensagem do HIPS
Servidor primário	Nome do ERA Server com o qual um cliente está se comunicando
Data de recebimento	Horário no qual o evento foi registrado pelo ERAS
Data de ocorrência	Horário no qual o evento ocorreu
Nível	Nível de emergência do evento
Aplicativo	Nome do aplicativo que gerou o log do HIPS. Ele tem o formato de um caminho UNC para o executável do aplicativo
Operação	Atividade detectada que afeta o aplicativo de destino
Destino	Arquivo do aplicativo que gerou o log do HIPS. Ele está no formato de um caminho para o arquivo na pasta de instalação do aplicativo
Ação	Ação que foi realizada pelo HIPS com base no modo/regra ativo atual

OBSERVAÇÃO: por padrão, o registro em log da atividade do HIPS está desabilitado. Para habilitar o registro em log dessa atividade ou alterar configurações, vá para **Ferramentas** > **Opções do servidor** > **Manutenção do servidor** > Parâmetros de coleta de log 95.

3.4.8 Log de controle do dispositivo

Esta guia mostra logs detalhados da atividade de Controle de dispositivo.

Atributo	Descrição
Id de controle de dispositivo	ID da entrada correspondente no banco de dados
Nome do cliente	Nome do cliente reportando o evento
Servidor primário	Nome do ERAS com o qual um cliente está se comunicando
Data de recebimento	Horário no qual o evento foi registrado pelo ERAS
Data de ocorrência	Horário no qual o evento ocorreu
Nível	Nível de alerta
Usuário	Nome do usuário associado ao evento
Grupo	Grupo ao qual o cliente que reportou a atividade pertence
Classe de dispositivo	Tipo do dispositivo removível (armazenamento USB, DVD...)
Dispositivo	Número de série (se disponível) e nome fornecido do dispositivo removível
Evento	Evento reportado pelo recurso de Controle de dispositivo
Ação	Ação realizada pelo recurso de segurança específico

OBSERVAÇÃO: por padrão, o registro em log da atividade de Controle de dispositivo está desabilitado. Para habilitar o registro em log dessa atividade ou alterar configurações, vá para **Ferramentas** > **Opções do servidor** > **Manutenção do servidor** > **Parâmetros de coleta de log** 95.

3.4.9 Log de controle na Web

Esta guia mostra logs detalhados da atividade de Controle na Web.

Atributo	Descrição
Id de Controle na Web	ID da entrada correspondente no banco de dados
Nome do cliente	Nome do cliente reportando o evento
Servidor primário	Nome do ERAS com o qual um cliente está se comunicando
Data de recebimento	Horário no qual o evento foi registrado pelo ERAS
Data de ocorrência	Horário no qual o evento ocorreu
Nível	Nível de alerta
Usuário	Nome do usuário associado ao evento
Grupo	Grupo ao qual o cliente que reportou a atividade pertence
URL	URL da página bloqueada
Máscara de URL	Máscara de URL da página bloqueada
Categoria de URL	Categoria de URL da página bloqueada
Ação	Ação realizada pelo recurso de segurança específico

OBSERVAÇÃO: por padrão, o registro em log da atividade de Controle na Web está desabilitado. Para habilitar o registro em log dessa atividade ou alterar configurações, vá para **Ferramentas** > **Opções do servidor** > **Manutenção do servidor** > **Parâmetros de coleta de log** 95.

3.4.10 Guia Log de antispam

Esta guia mostra toda a atividade relacionada a antispam.

Atributo	Descrição
ID de antispam	ID da entrada correspondente no banco de dados (a ID tem a forma: número de antispam)
Nome do cliente	Nome do cliente reportando spam como mensagem
Servidor primário	Nome do ERA Server com o qual um cliente está se comunicando
Data de recebimento	Horário no qual o evento foi registrado pelo ERAS
Data de ocorrência	Horário no qual o evento ocorreu
Remetente	Endereço de email do remetente da mensagem marcado como spam
Destinatários	Destinatário da mensagem marcada como spam
Assunto	Assunto da mensagem marcada como spam
Pontuação	Classificação de spam (a probabilidade de a mensagem ser spam) em percentual
Motivo	Motivo pelo qual essa mensagem foi marcada como spam

Ação	Ação realizada para essa mensagem

OBSERVAÇÃO: por padrão, o registro em log da atividade de antispam está desabilitado. Para habilitar o registro em log dessa atividade ou alterar configurações, vá para **Ferramentas** > **Opções do servidor** > **Manutenção do servidor** > Parâmetros de coleta de log 95.

3.4.11 Guia Log da lista cinza

Esta guia mostra toda a atividade relacionada à lista cinza.

Atributo	Descrição
Id da lista cinza	ID da entrada correspondente no banco de dados (a ID tem a forma: número de lista cinza)
Nome do cliente	Nome do cliente reportando o evento
Servidor primário	Nome do ERAS com o qual um cliente está se comunicando
Data de recebimento	Horário no qual o evento foi registrado pelo ERAS
Data de ocorrência	Horário no qual o evento ocorreu
Domínio HELO	Nome de domínio usado pelo servidor de envio para identificar-se no servidor de recepção
Endereço IP	Endereço IP do remetente da mensagem
Remetente	Endereço de email do remetente da mensagem
Destinatário	Endereço de email do destinatário da mensagem
Ação	Ação realizada pelo recurso de segurança específico
Tempo restante	Tempo restante antes de a mensagem ser rejeitada ou verificada e entregue

OBSERVAÇÃO: por padrão, o registro em log da atividade de lista cinza está desabilitado. Para habilitar o registro em log dessa atividade ou alterar configurações, vá para **Ferramentas** > **Opções do servidor** > **Manutenção do servidor** > Parâmetros de coleta de log 95.

3.4.12 Guia Log de rastreamento

Esta guia relaciona resultados de rastreamentos de computador sob demanda que foram iniciados remotamente, localmente em computadores clientes ou como tarefas agendadas.

Atributo	Descrição
Id de rastreamento	ID da entrada correspondente no banco de dados (a ID está na forma: número de rastreamento)
Nome do cliente	Nome do cliente no qual o rastreamento foi realizado
Nome do computador	Nome da estação de trabalho/servidor (nome de host)
Endereço MAC	Endereço MAC (adaptador de rede)
Servidor primário	Nome do ERA Server com o qual um cliente está se comunicando
Data de recebimento	Horário no qual o evento de rastreamento foi registrado pelo ERAS
Data de ocorrência	Horário no qual o rastreamento ocorreu no cliente
Alvos rastreados	Dispositivos, pastas e arquivos rastreados
Rastreado	Número de arquivos limpos
Infectado	Número de objetos infectados
Limpo	Número de objetos limpos (ou excluídos)
Status	Status do rastreamento
Usuário	Nome do usuário que foi identificado quando o incidente ocorreu
Tipo	Tipo de usuário
Scanner	Tipo de scanner
Detalhes	Status de envio do log do cliente

3.4.13 Guia Log de mobile

Esta guia exibe logs detalhados dos telefones celulares conectados ao ERA Server.

Atributo	Descrição
Id de celular	ID da rede do dispositivo móvel
Nome do cliente	Nome do cliente no qual a ação foi realizada
Nome do computador	Nome da estação de trabalho/servidor (nome de host)
Endereço MAC	Endereço MAC (adaptador de rede)
Servidor primário	Nome do ERA Server com o qual um cliente está se comunicando
Data de recebimento	Horário no qual o evento foi registrado pelo ERAS
Data de ocorrência	Horário no qual o evento ocorreu no cliente
Nível	Nível de alerta
Registrar tipo	Tipo de um log (p. ex., log de auditoria de segurança, log de antispam de SMS).
Evento	Descrição do evento
Tipo de objeto	Objeto ao qual o evento está relacionado (p. ex., SMS, arquivo, ...)
Nome do objeto	Objeto específico ao qual o evento está relacionado (p. ex., número de telefone do remetente de SMS, caminho para arquivo, ...)
Ação	Ação realizada (ou erro encontrado) durante o evento

3.4.14 Guia Quarentena

Esta guia consolida todas as entradas de quarentena em sua rede.

Atributo	Descrição
Id de quarentena	Número de ID do objeto em quarentena, atribuído em ordem de ocorrência
Hash	Código hash de arquivo
Data de recebimento	Horário no qual o evento de rastreamento foi registrado pelo ERAS
Ocorreu primeiro	Tempo decorrido da primeira ocorrência do item em quarentena
Última ocorrência	Tempo decorrido da ocorrência mais recente do item em quarentena
Nome do objeto	Geralmente, uma pasta na qual a infiltração está localizada
Nome do arquivo	Nome do arquivo em quarentena
Extensão	Tipo de extensão do arquivo em quarentena
Tamanho	Tamanho do arquivo em quarentena
Motivo	Motivo da quarentena - geralmente uma descrição do tipo de ameaça
Contagem de clientes	Número de clientes colocando o objeto em quarentena
Acessos	Número de vezes em que o objeto foi colocado em quarentena
Arquivo	Indica se foi solicitado download do objeto para o servidor

OBSERVAÇÃO: observe que os campos **Nome do objeto**, **Nome de arquivo** e **Extensão** mostra somente os primeiros três objetos. Para obter informações detalhadas, abra a janela Propriedades pressionando a tecla **F3** ou dando um duplo clique no item selecionado.

A quarentena centralizada fornece uma visão geral de arquivos em quarentena, que estão localmente armazenados nos clientes com uma opção para solicitá-los sob demanda. Quando um arquivo for solicitado, ele será copiado para o ERA Server de forma segura e criptografada. Por motivos de segurança, a criptografia é realizada no salvamento do arquivo para o disco. Para obter instruções sobre o trabalho com arquivos em quarentena, consulte o capítulo Tarefa de restauração/exclusão da quarentena 67.

OBSERVAÇÃO: a quarentena centralizada requer a instalação do EAV/ESS versão 4.2 ou mais recente em clientes.

3.4.15 Guia Tarefas

O significado dessa guia é descrito no capítulo intitulado Tarefas[64]. Os seguintes atributos estão disponíveis:

Atributo	Descrição
Estado	Status da tarefa (Ativo = sendo aplicada, Concluído = a tarefa foi entregue para os clientes)
Tipo	Tipo de tarefa
Nome	Nome da tarefa
Descrição	Descrição da tarefa
Data para implantação	Data/hora da execução da tarefa
Data de recebimento	Horário no qual o evento foi registrado pelo ERAS
Detalhes	Status de envio do log da tarefa
Comentário	Um breve comentário descrevendo o cliente (inserido pelo administrador)

3.4.16 Guia Relatórios

A guia **Relatórios** será usada para transformar informações estatísticas em gráficos ou diagramas. Eles podem ser salvos e processados posteriormente no formato Comma Separated Value (Valor separado por vírgulas) (*.csv*) usando ferramentas ERA para fornecer saídas gráficas e gráficos. Por padrão, o ERA salva a saída em formato HTML. A maioria dos relatórios relacionados a infiltrações são gerados do log de ameaças.

1. Modelos de painel[38] - modelos para os relatórios de dashboard na web. Um painel é um conjunto de relatórios que está disponível on-line usando um navegador. O layout de painel é totalmente personalizável para cada administrador. Dê um clique duplo em um modelo para exibir uma visualização do relatório usado no painel.
2. **Modelos de relatório** - modelos de relatórios estáticos. Na parte superior da janela do Console, na seção **Modelos de relatório**, você poderá ver os nomes de modelos que já foram criados. Ao lado dos nomes de modelo, você poderá encontrar informações sobre intervalos de tempo e quando os relatórios são gerados, de acordo com os modelos predefinidos. Você pode criar novos modelos ou editar modelos predefinidos existentes (mostrados a seguir):

- **Visão geral de clientes** - mostra os status de proteção de todos os clientes.
- **Clientes com ameaças ativas** - mostra clientes com ameaças ativas (ameaças que não foram limpas durante o rastreamento), junto com informações sobre as ameaças ativas.
- **Relatório abrangente de ataques à rede** - mostra um relatório abrangente sobre a atividade de ataques à rede.
- **Relatório abrangente de SMS** - mostra um relatório abrangente sobre a atividade de spam por SMS.
- **Relatório abrangente de SPAM** - mostra um relatório abrangente sobre a atividade de spam por email.
- **Relatório abrangente de ameaças** - mostra um relatório abrangente sobre todas as ameaças encontradas.
- **Resumo de informações personalizadas** - mostra um relatório abrangente com informações definidas pelo usuário (precisa ser definido primeiro).
- **Principais clientes problemáticos** - mostra clientes com o maior número e problemas (com base nos relatórios acima).

Clicar em **Modelos padrão** redefinirá os modelos predefinidos em seu estado original (essa ação não afetará modelos criados personalizados).

- **Opções**

Clique em **Gerar agora** (certifique-se de que a guia **Opções** esteja selecionada) para gerar um relatório a qualquer momento, independentemente do agendamento. Selecione o tipo de saída a partir do menu suspenso próximo a esta opção. Isso define o tipo de arquivo do relatório gerado (HTML, ZIP ou PDF).

Relatório

Tipo - tipo de relatório com base nos modelos predefinidos. Ele pode ser modificado para modelos predefinidos ou selecionado para os modelos personalizados criados. Clicar em **...** (ao lado dessa opção) mostra relatórios que podem ser usados para a opção **Relatório personalizado abrangente**.

Estilo - você pode modificar a cor e o layout do relatório usando esse menu suspenso.

Filtro

Clientes de destino - você pode especificar essa opção se quiser que o relatório colete **Todos** os dados ou os dados de **Somente clientes/servidores/grupos selecionados** ou poderá **Excluir clientes/servidores/grupos selecionados**. Os clientes/servidores/grupos podem ser especificados depois de clicar em **...** ao lado do menu suspenso **Clientes de destino**, na janela da caixa de diálogo **Adicionar**/**Remover**.

Ameaça - você também pode especificar se quiser que o relatório mostre **Todas as ameaças**, **Somente ameaças selecionadas** ou **Excluir ameaças selecionadas**. As ameaças podem ser especificadas depois de clicar em **...** ao lado desse menu suspenso na janela da caixa de diálogo **Adicionar**/**Remover**.

Outros detalhes podem ser configurados clicando-se em **Configurações adicionais...**. Essas configurações aplicam-se principalmente a dados no cabeçalho e nos tipos de diagramas gráficos usados. No entanto, você também pode filtrar dados de acordo com o status de atributos escolhidos, bem como escolher qual formato de relatório será usado (. html, .csv).

- **Intervalo**

Atual - somente eventos que ocorreram durante o período de tempo escolhido serão incluídos no relatório, p. ex., se um relatório for criado na quarta-feira e o intervalo for definido como Semana atual, então os eventos de domingo, segunda, terça e quarta serão incluídos.

Concluídos - somente eventos que ocorreram durante um período escolhido e encerrado serão incluídos no relatório (p. ex., o mês inteiro de agosto ou uma semana inteira de domingo até o próximo sábado). Se a opção **Adicionar também o período atual** for selecionada, o relatório incluirá eventos do último período encerrado até o momento da criação.

Exemplo:

Queremos criar um relatório, incluindo eventos da última semana do calendário, por exemplo, de domingo até o próximo sábado. Queremos que esse relatório seja gerado na quarta-feira seguinte (depois de sábado). Na guia **Intervalo**, selecione **Concluído** e **1 semana**. Remova a opção **Adicionar também o período atual**. Na guia **Agenda**, defina a **Frequência** como **Semanalmente** e selecione **Quarta-feira**. As outras configurações podem ser definidas a critério do administrador.

De/A - use essa configuração para definir um período para o qual o relatório será gerado.

- **Agenda**

Frequência - permite que você defina e configure um relatório automático por um período especificado ou em intervalos.

Depois de agendar o relatório, clique em **Selecionar alvo...** para especificar onde o relatório será salvo. Os relatórios podem ser salvos em ERAS (padrão), enviados por email para um endereço escolhido ou exportados para uma pasta. A última opção é útil se o relatório for enviado para uma pasta compartilhada na intranet de sua organização, onde ele poderá ser visualizado por outros funcionários. Se usar esta opção, selecione o tipo de arquivo de saída (HTML, ZIP ou PDF). Você pode usar variáveis (%) no caminho da pasta. As variáveis não diferenciam maiúsculas de minúsculas. Essas variáveis acrescentam informações personalizadas no relatório gerado. Se você acrescentar o símbolo "\" ao fim do caminho da pasta, os relatórios serão gravados diretamente nessa pasta e os dados serão substituídos. As seguintes variáveis são compatíveis:

Variável	Descrição
%INTERVAL%	O intervalo para o qual o relatório está sendo gerado, como retornado de CReport::GetIntervalString (INTERVALSTRING_FOLDER).
%DATE%	Data atual ("YYYY-MM-DD").
%TIME%	Hora atual ("HH-MM-SS").
%DATETIME%	Data e hora atuais ("YYYY-MM-DD HH-MM-SS").
%TIMESTAMP%	Data e hora atual, unixtime, em 8 dígitos hexadecimais.
%RND4%	Valor aleatório, 4 dígitos hexadecimais, praticamente exclusivo (não recomendado).
%DDATE%	Data atual, densa ("YYYYMMDD").
%DTIME%	Hora atual, densa ("HHMMSS").
%YEAR%, %MONTH%, %DAY%, %HOUR%, %MINUTE%, %SECOND%	Partes de data/hora atual como dígitos (4 para ano, 2 para outras).

%COUNTER%	Contador decimal de 5 dígitos, iniciando em 1.
%COUNTER1%, %COUNTER2%, %COUNTER3%, %COUNTER4%, %COUNTER5%	Contador decimal de 1/2/3/4/5 dígitos, iniciando em 1.
%CCOUNTER%	Contador condicional decimal de 5 dígitos (a primeira iteração é apagada, a segunda iteração será "00002")
%CCOUNTER1%, %CCOUNTER2%, %CCOUNTER3%, %CCOUNTER4%, %CCOUNTER5%	Contador condicional decimal de 1/2/3/4/5 dígitos.
%UCOUNTER%	Contador sublinhado decimal de 5 dígitos (a primeira iteração é apagada, a segunda iteração será "_00002")
%UCOUNTER1%, %UCOUNTER2%, %UCOUNTER3%, %UCOUNTER4%, %UCOUNTER5%	Contador sublinhado decimal de 1/2/3/4/5 dígitos.
%%	Sinal % individual.

Por exemplo, se você inserir o caminho na forma: *C:\Reports\%INTERVAL%_%COUNTER%*", os nomes de pasta serão gerados como *C:\Reports\Day 2012-02-02_00001; C:\Reports\Day 2012-02-02_00002* e assim por diante.

Para enviar relatórios gerados por email, você precisa inserir o servidor SMTP e informações de endereço do remetente em **Ferramentas** > **Opções do servidor** > **Outras configurações**.

3. **Relatórios gerados** - relatórios gerados anteriormente poderão ser visualizados na guia **Relatórios gerados**. Para mais opções, selecione relatórios individuais (ou vários) e use o menu de contexto (clique direito do mouse). Você pode classificar os relatórios pelo **Nome do relatório**, pela **Data** em que o relatório foi gerado, pelo **Nome do modelo** e pelo **Local** do relatório. Clique em **Abrir** ou dê um duplo clique em um relatório na lista para abrir o relatório. Clicar em um relatório na lista mostrará uma visualização na seção inferior (se essa opção for selecionada).

Os modelos inseridos na lista **Favoritos** poderão ser usados posteriormente para gerar imediatamente novos relatórios. Para mover um modelo para Favoritos, clique com o botão direito do mouse no relatório e selecione **Adicionar a favoritos** no menu de contexto.

3.4.16.1 Painel

Um **Painel** é um conjunto de relatórios que são automaticamente atualizados com novos dados, que fornecem um visão geral abrangente do estado do sistema. Cada usuário com acesso ao ERAC e um login tem um conjunto individual de painéis que eles podem personalizar totalmente. Essas configurações são armazenadas diretamente no servidor; portanto, o usuário tem acesso ao mesmo painel de qualquer navegador.

O recurso de painel usa o servidor HTTP ERA por padrão, comunicando-se através da porta 443. As portas e os certificados (para HTTPS) podem ser alterados em **Opções avançadas do servidor** no Console do ERA. As opções **Painel** e **Opções de conexão de painel** também podem ser acessadas da janela principal do programa ERAC na barra de ferramentas (ícone de nuvem azul).

OBSERVAÇÃO: o administrador precisa preparar um modelo para cada relatório para que ele possa ser usado no painel. Caso contrário, os dados nos relatórios poderão não ser exibidos corretamente.

OBSERVAÇÃO: Por padrão, o **Painel** será iniciado usando o protocolo https com um certificado assinado automaticamente. Isso pode acionar a seguinte mensagem de aviso no navegador: *O certificado de segurança apresentado por este site não foi emitido por uma autoridade de certificado confiável*. Observe que ao usar HTTP, seus nomes de usuário e senhas serão transmitidos em texto sem formatação. Isso pode ser especialmente perigoso ao usar logins do Windows/domínio.

O instalador pode gerar um certificado assinado automaticamente para você. Alguns navegadores podem exibir um aviso ao encontrar um certificado assinado automaticamente. Você também pode fornecer seu próprio certificado durante o modo de instalação avançada ou a qualquer momento posteriormente pelo ESET Configuration Editor. O certificado fornecido pode ser assinado por uma autoridade de certificado confiável ou usando sua própria raiz de certificado. O seguinte certificado X.509 e formatos de chave privada são compatíveis:

- ASN - certificado com codificação DER ASN.1 e chave em arquivos separados.
- PEM - certificado ASN com codificação Base64 e chave em arquivos separados.
- PFX - certificado e chave privada em um único arquivo de contêiner.

Não é possível usar um certificado e uma chave em formatos diferentes. Você pode alterar o protocolo para http clicando em **Painel** (ícone de nuvem azul) na janela principal do programa do ERAC e então **Configurar...** ou pode

definir seu próprio certificado (em formato de arquivo PEM, com codificação base64 X.509) usando o ESET Configuration Editor (**Ferramentas** > **Servidor** > **Opções** > **Avançadas** > **Editar configurações avançadas...** > **Administrador remoto** > **ERA Server** > **Configurações** > **Painéis** > **Chave de certificado local**/**Certificado local**).

OBSERVAÇÃO: o painel também é compatível com o protocolo IPv6. Por exemplo, *http://[::1]:8080*.

Há um conjunto de modelos predefinidos (mostrado a seguir) para o **Painel** ou você pode criar um modelo personalizado.

- **Resumo de ação antispam** - mostra um resumo de toda a atividade do mecanismo antispam.
- **Composição de pontuação antispam** - mostra a composição da pontuação antispam e o número de mensagens classificadas.
- **Visão geral da conexão do cliente** - mostra uma visão geral de conexões clientes com base no horário e no status de sua conexão.
- **Resumo de informações personalizadas de cliente 1** - mostra um relatório abrangente com informações definidas pelo usuário (precisa ser definido primeiro).
- **Resumo de informações personalizadas de cliente 2** - mostra um relatório abrangente com informações definidas pelo usuário (precisa ser definido primeiro).
- **Resumo de informações personalizadas de cliente 3** - mostra um relatório abrangente com informações definidas pelo usuário (precisa ser definido primeiro).
- **Clientes de grupos** - mostra a contagem de clientes de grupos selecionados.
- **Clientes de grupos para todos** - mostra a proporção de contagem de clientes de grupos selecionados para a contagem total de clientes em geral (como um percentual).
- **Clientes com ameaças ativas** - mostra clientes com ameaças ativas (não limpas durante o rastreamento), junto com informações sobre as ameaças ativas.
- **Resumo de ação de lista cinza** - mostra todas as mensagens em lista cinza e a ação realizada.
- **Computadores gerenciados e não gerenciados** - mostra computadores que estão atualmente se conectando ao ERA Server (computadores gerenciados) e computadores que não são (computadores não gerenciados). Isso é baseado na tarefa de pesquisa padrão.
- **Resumo do nome de SO** - mostra o número e o tipo de sistemas operacionais clientes.
- **Resumo do nome de SO** - mostra o número e o tipo de produtos de segurança clientes.
- **Resumo do status de proteção** - mostra o número e o tipo de clientes e seu status de segurança.
- **Progresso de spam SMS** - mostra o progresso de spam SMS.
- **Carga do banco de dados do servidor** - mostra a quantidade de tempo total em que o banco de dados foi usado por todas as ameaças.
- **Consultas de banco de dados de servidor** - mostra a quantidade de consultas SQL realizadas no banco de dados.
- **Carga de hardware do servidor** - mostra o uso de CPU e RAM da máquina do servidor.
- **Monitoramento de status do servidor** - mostra o status do servidor junto com informações sobre a atualização do banco de dados de vírus.
- **Progresso comparativo de ameaças** - progresso de eventos de malware por ameaças selecionadas (usando filtro) em comparação com o número total de ameaças.
- **Progresso de ameaças** - progresso de eventos de malware (número).
- **Ameaças por objeto** - número de alertas de ameaça de acordo com o vetor de ataque (emails, arquivos, setores de inicialização).
- **Ameaças por scanner** - número de alertas de ameaça dos módulos de programa individual.
- **Principais clientes por desconexão** - mostra os principais clientes classificados por sua última data de conexão.
- **Principais clientes com a maioria dos ataques à rede** - Mostra os principais clientes com a maioria dos ataques à rede.
- **Principais clientes com a maioria dos ataques à rede** - mostra os principais clientes com a maioria de spam por SMS.
- **Principais clientes com a maioria do spam** - mostra os principais clientes com a maioria das mensagens de spam.
- **Principais clientes com a maioria das ameaças** - relaciona a maioria das estações de trabalho clientes "ativas" (mensuradas pelo número de ameaças detectadas).
- **Principais destinatários de email de lista cinza** - mostra os principais destinatários de mensagens de lista cinza.
- **Principais remetentes de email de lista cinza** - mostra os principais remetentes de mensagens de lista cinza.
- **Principais ataques à rede** - Mostra os principais ataques à rede.
- **Principais fontes de ataques à rede** - Mostra as principais fontes de ataques à rede.
- **Principais remetentes de spam SMS** - mostra os principais remetentes de spam SMS para destinos especificados.
- **Principais destinatários de spam** - mostra os principais destinatários de mensagens de spam.
- **Principais remetentes de spam** - mostra os principais remetentes de mensagens de spam.
- **Principais ameaças** - lista das ameaças mais frequentemente detectadas.
- **Principais ameaças por propagação** - Mostra as principais ameaças por propagação.
- **Principais usuários com a maioria das ameaças** - relaciona a maioria dos usuários "ativos" (mensurados pelo número de ameaças detectadas).
- **Computadores não registrados** - mostra todos os computadores não gerenciados - computadores que não estão se conectando ao ERA Server. Essa opção também mostra o horário no qual um novo computador não gerenciado foi encontrado.

Os modelos de relatórios existentes podem ser importados/exportados de/para um arquivo *.xml* ao clicar em **Importar.../Exportar...**. . Os conflitos de nome durante a importação (modelos existentes e importados com o mesmo

nome) são resolvidos ao atribuir uma cadeia de caracteres aleatória após o nome de um modelo importado.

Para salvar as configurações de relatórios definidos em um modelo, clique em **Salvar** ou **Salvar como...**. Se você estiver criando um novo modelo, clique em **Salvar como...** e dê ao modelo um nome. Clicar em **Modelos padrão** redefinirá os modelos predefinidos em seu estado original (essa ação não afetará modelos criados personalizados).

- **Opções**

Visualizar relatório - clicar nesse botão gerará o painel e mostrará uma visualização.

Relatório

Tipo - tipo de relatório com base nos modelos predefinidos. Ele pode ser modificado para modelos predefinidos que foram usados para a criação de modelos personalizados.

Filtro

Clientes de destino - você pode especificar essa opção se quiser que o relatório colete **Todos** os dados ou os dados de **Somente clientes/servidores/grupos selecionados** ou poderá **Excluir clientes/servidores/grupos selecionados**. Os clientes/servidores/grupos podem ser especificados depois de clicar no botão **...** ao lado do menu suspenso **Clientes de destino**, na janela da caixa de diálogo **Adicionar/Remover**.

Ameaça - você também pode especificar se quiser que o relatório mostre **Todas as ameaças**, **Somente ameaças selecionadas** ou **Excluir ameaças selecionadas**. As ameaças podem ser especificadas depois de clicar em **...** ao lado desse menu suspenso na janela da caixa de diálogo **Adicionar/Remover**.

Outros detalhes podem ser configurados clicando-se em **Configurações adicionais...**. Essas configurações aplicam-se principalmente a dados no cabeçalho e nos tipos de diagramas gráficos usados. No entanto, você também pode filtrar dados de acordo com o status de atributos selecionados. Você também pode selecionar qual formato de relatório será usado (.html, .csv).

- **Intervalo**

Tempo- **Últimos X minutos/horas/dias/semanas/meses/anos** a partir dos quais deseja que os dados sejam incluídos no relatório. O tempo é baseado no horário no qual o incidente foi reportado ao ERA.

- **Atualizar**

Intervalo de atualização do navegador - selecione o intervalo de tempo para a atualização de novos dados recebidos do servidor da web.

Intervalo de atualização do servidor- selecione o intervalo de tempo durante o qual os dados serão enviados para o servidor da web.

3.4.16.1.1 Lista de servidores da web de painel

Clique na seta ao lado do ícone Painel no menu principal para configurar as opções de conexão **Servidores da web de painel**.

- **Servidores da web de painel** - lista de todos os servidores da web de painel disponíveis.
- **Remover** - clicar nesse botão removerá da lista o servidor da web de painel selecionado.
- **Definir como padrão** - define o servidor da web de painel selecionado como padrão. Essa opção será a primeira disponível no menu suspenso (depois de clicar na seta ao lado do ícone de painel) e será a primeira aberta depois de clicar no próprio ícone de painel.
- **Protocolo** - você poderá escolher entre http e https com um certificado autoassinado.
- **Nome do host ou endereço IP** - exibe o nome do host ou o endereço IP do servidor da web do painel selecionado. Como alternativa, você pode inserir um novo nome do host ou endereço IP e clicar em **Adicionar/salvar** para salvar os dados e adicionar o servidor da web do painel à lista.
- **Comentário** - comentário/descrição opcional do servidor da web do painel selecionado.

OBSERVAÇÃO: o painel também é compatível com o protocolo IPv6. Por exemplo, *http://[::1]:8080*.

3.4.16.2 Cenário de relatório de exemplo

Para manter a segurança de rede de seus clientes no nível máximo, você precisará ter uma boa visão geral do status de segurança da rede. Você poderá criar facilmente relatórios com detalhes completos sobre ameaças, atualizações, versões de produto cliente, etc. (para obter mais informações, consulte a seção Relatórios 36). Geralmente, um relatório semanal fornecerá todas as informações necessárias. No entanto, poderá haver situações durante as quais será necessário vigilância adicional, como na hipótese de uma ameaça encontrada.

Para fornecer um exemplo, criaremos um grupo paramétrico intitulado *Quarentena*. Esse grupo conterá somente computadores nos quais uma ameaça foi detectada e limpa durante o rastreamento sob demanda mais recente. Defina essa condição ao marcar a caixa de seleção ao lado de **TEM Último rastreamento detectou ameaça**. Para criar esse grupo paramétrico, siga as instruções na seção Grupos paramétricos 70.

OBSERVAÇÃO: ao criar o grupo *Quarentena*, verifique se a opção **Adesivo** está desabilitada. Isso garante que o computador será atribuído dinamicamente e removido assim que as condições não forem mais atendidas.

Crie o relatório *Colocar computadores em quarentena*. Para criar um relatório para esse grupo paramétrico, siga as instruções na seção Relatórios 36.

As configurações específicas para nosso exemplo são as seguintes:

- Configurações da seção **Opções**:

Tipo: Relatório de quarentena com detalhes
Estilo: Esquema azul
Clientes de destino: Somente grupos selecionados
Ameaça: n/d

- Configurações de caractere curinga de **Intervalo**:

Atual: Dia

- Configurações de caractere curinga de **Agenda**:

Frequência: Diariamente
A cada: 1 dia

DICA: você pode armazenar resultados no banco de dados de relatório ou definir uma pasta na qual as cópias do relatório serão armazenadas. Os relatórios também poderão ser enviados por email. Todas essas configurações estão disponíveis depois de clicar em **Selecionar destino...**.

Os relatórios gerados podem ser visualizados no caractere curinga de **Relatórios gerados** na seção **Relatórios**.

Resumo: criamos o grupo paramétrico *Quarentena*, contendo computadores nos quais uma ameaça foi reportada durante o rastreamento sob demanda mais recente. Em seguida, criamos um relatório automatizado que nos informará, diariamente, quais computadores pertencem ao grupo *Quarentena*, nos fornecendo uma boa visão geral do status de nossa rede de cliente, a fim de que possamos manter possíveis ameaças sob controle.

DICA: se você quiser ver os detalhes de log do último rastreamento, poderá usar o tipo de relatório **Relatório de rastreamentos com detalhes**.

3.4.17 Guia Instalação remota

Esta guia fornece opções para vários métodos de instalação remota do ESET Smart Security ou do ESET NOD32 Antivirus em clientes. Para obter informações detalhadas, consulte o capítulo Instalação remota 53.

1. Para pesquisar computadores, você poderá usar a tarefa de pesquisa padrão ou criar uma nova. Para criar uma nova tarefa de pesquisa, clique em **Nova pesquisa...** para iniciar o Assistente de tarefa de pesquisa de rede 43. Para executar uma tarefa de pesquisa, clique em **Executar**.

2. Os resultados de pesquisa podem ser filtrados usando a ferramenta **Filtro de resultados da pesquisa** na seção a seguir. Filtrar os resultados não afetará a tarefa de pesquisa real. Critérios adicionais de pesquisa:

- **Computadores não registrados** - mostra computadores que não estão relacionados no banco de dados de servidor atual.
- **Clientes com aviso de última conexão** - mostra computadores que estão relacionados no banco de dados de servidor atual e têm o aviso de última conexão.
- **Ocultar computadores ignorados** por padrão, esta opção está ativada. Essa opção oculta computadores na lista ignorar criada pelo administrador (no menu de contexto, também é possível editar e importar essa lista).

3. Os resultados de pesquisa da tarefa de pesquisa atual são mostrados na seção principal **Computador**. Daqui, você pode gerenciar pacotes de instalação 44 e executar a Instalação forçada remota 55 usando o menu de contexto.

O menu de contexto (clique direito do mouse) da guia **Computadores** oferece as seguintes opções:

- **Gerenciar pacotes** - executa o **Editor do pacote de instalação**. Consulte Instalação remota 44 para obter detalhes.
- **Cliente Windows de atualização** - execute a tarefa de atualização. Use essa opção se quiser instalar uma versão mais recente do ESS/EEV para substituir uma mais antiga.
- **Diagnóstico de instalação forçada do Windows** - verifica a disponibilidade de clientes e serviços a serem usados durante a instalação remota. Para obter mais informações, consulte o capítulo intitulado Diagnóstico de instalação remota 46.
- **Instalação forçada do Windows** - executa a instalação forçada remota 55 do Windows.
- **Instalação forçada do Linux/Mac Push** - executa a instalação forçada do Linux/Mac. Consulte os Requisitos para instalação forçada de Linux/Mac 55 para mais detalhes.
- **Exportar para pasta ou script de logon** - consulte Instalação remota por logon/email 57 para obter detalhes.
- **Enviar por email** - consulte Instalação remota por logon/email 57 para obter detalhes.
- **Definir logon padrão para instalações de script de logon e email** - abre a janela **Logon padrão**, na qual você pode especificar o nome de usuário e senha de uma conta de administrador para os computadores de destino.
- **Propriedades** - abre a janela **Propriedades do cliente** na qual você pode encontrar todas as informações importantes sobre um cliente.

Para as outras opções de menu de contexto, consulte o capítulo menu de contexto 27.

3.4.17.1 Assistente de tarefa de pesquisa de rede

Uma **tarefa de pesquisa** é um conjunto de parâmetros usados para pesquisar sua rede de computadores. Tarefas de pesquisa criadas são armazenadas diretamente no servidor; portanto, estão disponíveis para todos os administradores.

Você pode usar a tarefa de pesquisa padrão predefinida, que é executada periodicamente (ela também pode ser acionada manualmente) e pesquisa a rede inteira. Os resultados de pesquisa dessa tarefa são armazenados no servidor. Essa tarefa também pode ser editada, mas depois de iniciada ela não poderá ser interrompida até ser concluída.

Os parâmetros de tarefa personalizada são armazenados no servidor, mas seus resultados de pesquisa são enviados somente para o console do qual foram executados. Essas tarefas de pesquisa podem ser iniciadas somente manualmente.

1. Primeiro, escolha o tipo de tarefa de rede:

- **Modelo de rastreamento de rede** - cria uma nova tarefa de pesquisa com um nome e um conjunto de parâmetros que serão armazenados no servidor para reutilização. Os resultados de pesquisa não são armazenados. Executar uma nova pesquisa atualizará a lista de computadores clientes atualmente disponíveis em sua rede.
- **Tarefa de pesquisa de rede temporária** - cria uma tarefa de pesquisa temporária, que não é armazenada no servidor e será excluída depois do encerramento de sua sessão atual.

2. Em seguida, escolha os métodos a serem usados para pesquisar a rede (você pode escolher vários métodos de pesquisa):

- **Pesquisa do Active Directory** - essa opção permite que você selecione as ramificações do Active Directory nas quais você deseja pesquisar por computadores; você também pode **Incluir computadores desativados**.
- **Rede do Windows (Wnet)** - pesquisa os computadores em sua rede do Windows.
- **Shell** - pesquisa todos os computadores em seus locais de rede (vizinhança de rede do Windows).
- **Pesquisa de endereço IP** - permite que você selecione o **Intervalo IP/máscara IP** a ser usado durante a pesquisa ou pode definir uma **lista personalizada de endereço IP**. Os computadores são pesquisados acessando suas portas (que podem ser configuradas). Você também pode usar um ping (isso é especialmente recomendado ao pesquisar computadores Linux).
- **Pesquisa de lista personalizada de computadores** - importe uma lista personalizada de computadores, o Assistente de tarefa de pesquisa de rede aceita listas no formato de arquivo *.txt.

Clicar em **Concluir** salvará a nova tarefa de pesquisa, temporariamente (tarefa de pesquisa de rede temporária) ou definitivamente (modelo de rastreamento de rede). Para concluir e iniciar a tarefa imediatamente, clique em **Concluir e executar**. Para executar a tarefa, clique em **Executar** na guia **Instalação remota**.

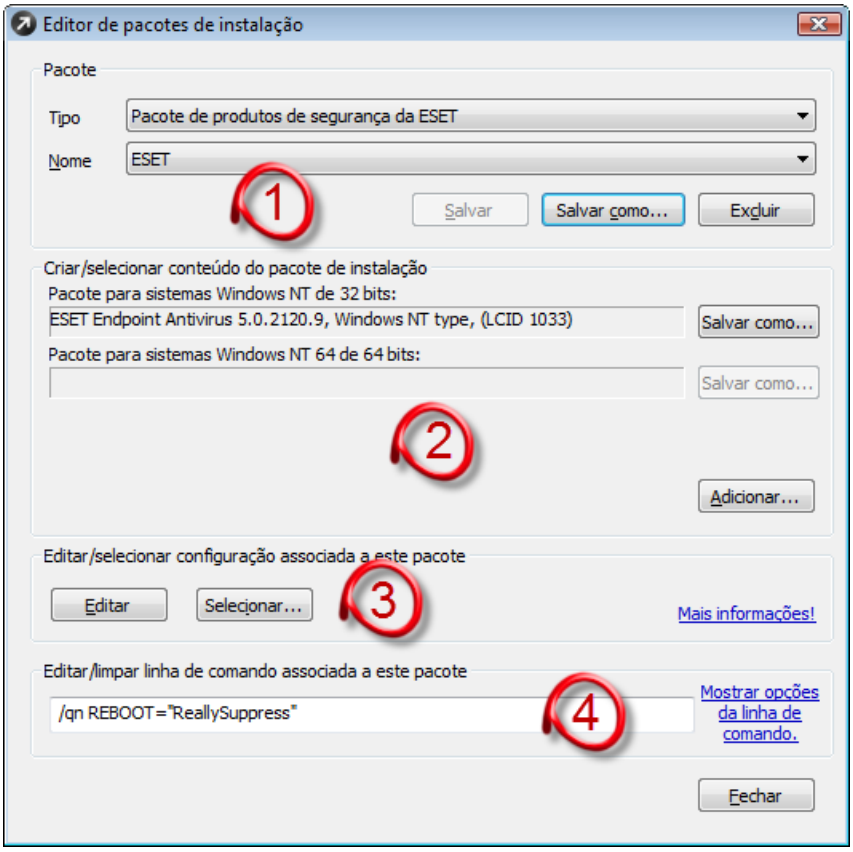
OBSERVAÇÃO: se o serviço estiver em execução na conta de sistema local, nenhum computador poderá ser encontrado usando a pesquisa Shell e Wnet. Isso ocorre porque a conta de sistema local não tem as permissões para realizar essa pesquisa. Para resolver isso, altere usuários ou use outro método de pesquisa.

3.4.17.2 Pacotes de instalação

A instalação remota é iniciada através do ERAC, mas o pacote de instalação está localizado no ERAS no seguinte diretório:

%ALLUSERSPROFILE%\Application Data\Eset\ESET Remote Administrator\Server\packages

Para lançar os pacotes de instalação através do ERAC, clique na guia **Instalação remota** e selecione a guia **Computadores**. Clique com o botão direito do mouse em qualquer lugar selecione **Gerenciar pacotes** no menu de contexto. A janela **Editor de pacotes de instalação** será aberta.



Cada pacote de instalação será definido por um Nome (veja (1) na figura acima). As seções restantes da janela da caixa de diálogo estão relacionadas ao conteúdo do pacote, que é aplicado depois que ele tiver sido entregue com êxito a uma estação de trabalho de destino. Cada pacote contém:

- Arquivos de instalação da solução cliente da ESET (**2**)
- Arquivo de configuração *.xml* para soluções cliente da ESET (**3**)

Observação: Quando criar um novo pacote de instalação, a senha primária do servidor para se conectar ao seu ERA Server será deixada em branco. Clique em **Editar** para editar a configuração .xml para este pacote e definir a senha (se necessário) na ramificação **Administração remota** do respectivo produto.

- Parâmetros da linha de comando atribuídos ao pacote (**4**)

O menu suspenso **Tipo** na seção (1) fornece acesso a recursos adicionais do ERA. Além da instalação remota, os produtos de segurança da ESET podem ser desinstalados remotamente usando a opção **Desinstalar produtos de segurança da ESET para Windows e NOD32 versão 2**. A instalação remota de um aplicativo externo também pode ser realizada selecionando-se **Pacote personalizado**. Isso é especialmente útil se você quiser executar vários scripts e executáveis na máquina do cliente, incluindo ferramentas de desinstalação para produtos de segurança de terceiros ou ferramentas autônomas de limpeza. Você pode especificar parâmetros personalizados da linha de comando para uso pela opção **Arquivo de entrada de pacote**. Para obter mais detalhes, consulte a Instalação de produtos de terceiros

usando o ERA 138.

Cada pacote recebe automaticamente um agente ESET Remote Installer, que permite instalação e comunicação perfeitas entre estações de trabalho clientes e o ERAS. O agente ESET Remote Installer é nomeado *einstaller.exe* e contém o nome do ERAS, bem como o nome e o tipo de pacote ao qual pertence. A seção a seguir fornece uma descrição detalhada do agente do instalador.

Há vários parâmetros que podem afetar o processo de instalação. Eles podem ser usados durante a instalação direta com o administrador presente na estação de trabalho ou para instalação remota. Para instalações remotas, os parâmetros são selecionados durante o processo de configuração de pacotes de instalação - parâmetros selecionados serão então aplicados automaticamente em clientes de destino. Parâmetros adicionais para ESET Smart Security e ESET NOD32 Antivirus poderão ser digitados depois do nome do pacote de instalação *.msi* (p. ex., *eav_nt64_ENU.msi /qn*):

- **/qn** - modo de instalação silenciosa - não são exibidas janelas de caixa de diálogo.
- **/qb!** - não é possível intervenção do usuário, mas o progresso de instalação é indicado pela barra de progresso em %.
- **REBOOT ="ReallySuppress"** - suprime a reinicialização depois da instalação do programa.
- **REBOOT ="Force"** - reinicia automaticamente depois da instalação.
- **REMOVE=...** - desabilita a instalação de um componente selecionado. Parâmetros de comando para cada componente estão listados abaixo:

  Emon - proteção do cliente de email
  Antispam - proteção antispam
  Dmon - proteção de documentos
  ProtocolScan - filtragem de protocolos
  Firewall - firewall pessoal
  eHttpServer - servidor de atualização de imagem
  eDevmon - controle de dispositivo
  MSNap - Microsoft NAP
  eParental - Controle de Web

- **REBOOTPROMPT =""** - depois da instalação, uma janela da caixa de diálogo solicitando que o usuário confirme a reinicialização será exibida (não pode ser usada junto com */qn*).
- **ADMINCFG ="path_to_xml_file"** - durante a instalação, os parâmetros definidos nos arquivos .xml especificados são aplicados a produtos de segurança da ESET. Este parâmetro não é necessário para instalação remota. Os pacotes de instalação contêm sua própria configuração *.xml*, que é aplicada automaticamente.
- **PASSWORD="password"** - Adicione esse parâmetro se as configurações do ESS/EAV forem protegidas por senha.

Os parâmetros para o ESET NOD32 Antivirus 2.x devem ser digitados depois do nome de arquivo *setup.exe*, que podem ser extraídos junto com outros arquivos do pacote de instalação (p. ex., *setup.exe /silentmode*):

- **/SILENTMODE** - modo de instalação silenciosa - não são exibidas janelas de caixa de diálogo.
- **/FORCEOLD** - instalará uma versão anterior em uma versão mais recente instalada.
- **/CFG ="path_to_xml_file"** - durante a instalação, os parâmetros definidos nos arquivos *.xml* especificados são aplicados a soluções clientes da ESET. O parâmetro não é necessário para instalação remota. Os pacotes de instalação contêm sua própria configuração *.xml*, que é aplicada automaticamente.
- **/REBOOT** - reinicia automaticamente depois da instalação.
- **/SHOWRESTART** - Depois da instalação, uma janela da caixa de diálogo solicitando que o usuário confirme a reinicialização será exibida. Esse parâmetro pode ser usado somente se combinado com o parâmetro *SILENTMODE*.
- **/INSTMFC** - instala bibliotecas MFC para o sistema operacional Microsoft Windows 9x, que são necessárias para que o ERA funcione corretamente. Esse parâmetro sempre pode ser usado, mesmo se as bibliotecas MFC estiverem disponíveis.

OBSERVAÇÃO: Se o UAC estiver habilitado em suas soluções clientes, as configurações de segurança de UAC padrão no Windows Vista/7/2008 exigirão uma confirmação de usuário antes da execução de qualquer programa. Tentar instalar remotamente soluções clientes e usar qualquer um dos parâmetros acima poderá resultar em uma janela pop-up no cliente exigindo interação do usuário. Para evitar interação do usuário, execute a instalação usando o seguinte comando: *C:\Windows\System32\msiExec.exe -i path_to_the_msi_file /qb! ADMINCFG="path_tp_the_xml_file" REBOOT="ReallySupress"* where *C:\Windows\System32\msiExec.exe -i* é o executável do componente do instalador do Windows e o parâmetro de instalação, e *path_to_the_msi_file /qb! ADMINCFG="path_tp_the_xml_file"*

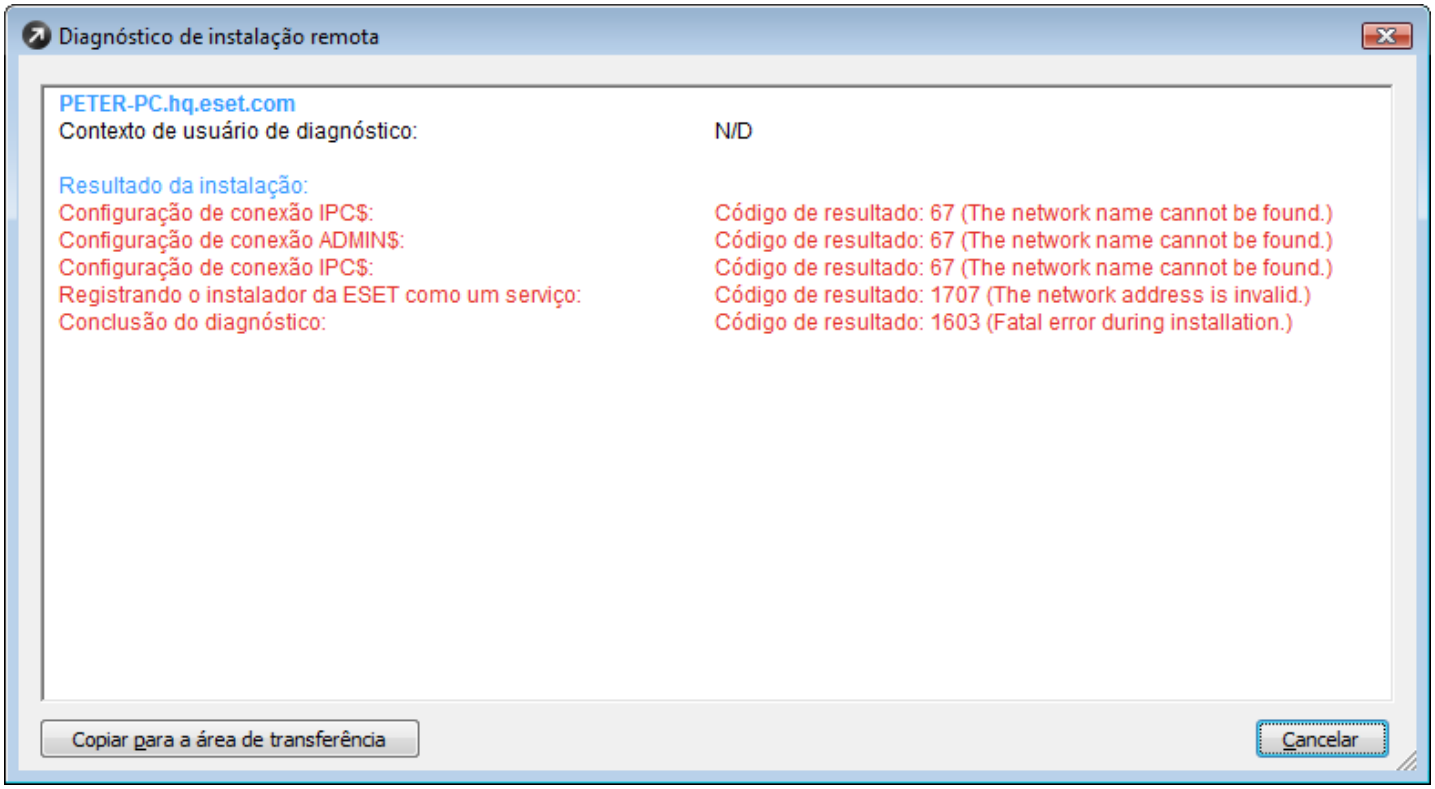
REBOOT="ReallySupress" é o caminho para o arquivo de instalação, bem como o arquivo de configurações do produto de segurança seguido pelo parâmetro de supressão da interação do usuário.

Em **Criar/selecionar conteúdo do pacote de instalação** (2), o administrador poderá criar um pacote de instalação autônoma com uma configuração predefinida de um pacote de instalação salvo e já existente (o botão **Salvar como...**). Esses pacotes de instalação podem ser executados manualmente na estação de trabalho cliente na qual o programa será instalado. O usuário precisa apenas executar o pacote e o produto será instalado, sem se conectar novamente com o ERAS durante a instalação.

OBSERVAÇÃO: Adicionar uma configuração ao arquivo de instalação *.msi* significa que a assinatura digital desse arquivo não será mais válida.

Importante: no Microsoft Windows Vista e em versões posteriores, recomendamos extremamente que você realize uma instalação remota silenciosa (o parâmetro */qn*, */qb*). Caso contrário, a interação com um usuário poderá causar falha na instalação remota devido a limite de tempo atingido.

3.4.17.3 Diagnóstico de instalação remota


Diagnóstico de instalação remota
PETER-PC.hq.eset.com
Contexto de usuário de diagnóstico:
N/D
Resultado da instalação:
Configuração de conexão IPC$:
Código de resultado: 67 (The network name cannot be found.)
Configuração de conexão ADMIN$:
Código de resultado: 67 (The network name cannot be found.)
Configuração de conexão IPC$:
Código de resultado: 67 (The network name cannot be found.)
Registrando o instalador da ESET como um serviço:
Código de resultado: 1707 (The network address is invalid.)
Conclusão do diagnóstico:
Código de resultado: 1603 (Fatal error during installation.)
Copiar para a área de transferência
Cancelar

- **Configuração de conexão IPC$**:

  O administrador deve ter permissões de administrador local em todos os computadores clientes.

  Os recursos compartilhados devem ser instalados e habilitados no cliente.

  O firewall de rede deve ter os recursos compartilhados habilitados (portas 445 e 135-139).

  A senha de administrador do Windows não pode estar em branco.

  A opção "Usar compartilhamento de arquivos simples" não pode ser ativada em um ambiente misto de grupos de trabalho e domínios.

  Certifique-se de que o serviço Server esteja sendo executado na máquina cliente.

- **Conexão de registro remoto (informações de SO)**:

  O serviço de registro remoto deve ser habilitado e iniciado no cliente.

- **Abertura de registro remoto (informações de SO)**:

  Acima + O administrador deve ter permissões de controle total em relação ao registro do cliente.

- **Leitura de registro remoto (informações de SO)**:

  O administrador deve ter permissões de leitura em relação ao registro do cliente. Se a operação acima for

concluída com êxito, essa operação também deverá ter êxito.

- **Conexão de registro remoto (Informações de produto de segurança da ESET)**:

  O administrador deve ter permissões de controle total do HKEY_LOCAL_MACHINE/SOFTWARE/ESET (ou a ramificação HKEY_LOCAL_MACHINE/SOFTWARE inteira).

- **Abertura de registro remoto (Informações de produto de segurança da ESET)**:

  Certifique-se de que o serviço de registro remoto esteja em execução no computador cliente.

- **Configuração de conexão ADMIN$**:

  O compartilhamento administrativo ADMIN$ deve estar habilitado.

- **Copiando instalador da ESET**:

  As portas 2222, 2223 e/ou 2224 devem ser abertas no servidor e devem ser permitidas no firewall de rede.

- **Configuração de conexão IPC$**:

  Se essa operação tiver sido concluída com êxito no diagnóstico de obtenção de informações, ela deverá ser concluída com êxito aqui.

- **Registrando o instalador da ESET como um serviço**:

  Certifique-se de que você tenha direitos suficientes para executar o installer.exe nos computadores de destino.

OBSERVAÇÃO: se houver um erro durante o diagnóstico, você poderá começar a resolver problemas com base nessas informações. Consulte o capítulo Requisitos 54 antes da instalação e o capítulo Códigos de erros frequentemente encontrados 132 para analisar códigos de erro.

3.4.17.4 Tarefas de instalação

A guia **Tarefas de instalação** da guia **Instalação remota** contém uma lista de tarefas e seus atributos. Nessa opção, você pode modificar o número de itens a serem visualizados e também clicar com o botão direito do mouse nas tarefas na lista para opções de gerenciamento/manutenção. Use o menu suspenso **Itens a serem exibidos** para aumentar/diminuir o número de itens visualizados por página, bem como os botões de navegação adjacentes para alternar entre as páginas disponíveis.

Você também pode filtrar as informações mostradas na guia Tarefas de instalação. Marque a opção **Usar filtro** no painel esquerdo para ativar o filtro. Em seguida, defina os Critérios de filtro de tarefas - **Somente clientes como (?,*)**/**Excluir clientes como (?,*)**. Digite o nome do computador no campo **Nome do computador:** ; você também pode usar caracteres curinga; por exemplo: *Com* e não a palavra inteira Computador. Clicar no botão **Redefinir** excluirá os critérios de filtro e desativará o filtro.

- **Nome da tarefa** - o nome da tarefa, para tarefas predefinidas, é o mesmo que tipo de tarefa.
- **Tipo de tarefa** - tipo da tarefa. Para obter mais informações, consulte o capítulo Tarefas 64.
- **Estado** - status de conclusão atual da tarefa.
- **Descrição** - breve descrição da ação da tarefa.
- **Data para implantação** - horário para/passado da execução da tarefa.
- **Data de recebimento** - horário para/passado da recepção da tarefa em seu ponto de execução.
- **Comentário** - observação atribuída à tarefa de instalação.

Dar um duplo clique em uma tarefa de instalação mostrará a janela **Propriedades**.

3.5 Opções do ERA Console

O ERA Console pode ser configurado no menu **Ferramentas** > **Opções do console...**.

3.5.1 Conexão

Para acessar as configurações do ERA Console, acesse o menu principal do ERAC menu **Ferramentas** > **Opções do console...** ou **Arquivo** > **Editar conexões...**. Essa guia é usada para configurar a conexão do ERAC para o ERAS. Para obter mais informações, consulte o capítulo Conectando-se ao ERAS 23.

A guia **Conexão** permite que você selecione a qual servidor você deseja se conectar e se deseja se conectar a esse servidor selecionado na inicialização do ERA Console. O console pode ser conectado somente a um servidor por vez. Se você quiser adicionar servidores replicados, precisará configurar a replicação no menu Ferramentas/Opções do servidor/Configurações de replicação... 99

OBSERVAÇÃO: a porta para se conectar ao ERA Server pode ser personalizada em **Ferramentas** > **Opções do servidor** > **Outras configurações** (consulte o capítulo Outras configurações 105).

Adicionar/Remover... - **use essa opção para** adicionar novos ERA Servers ou modificar servidores existentes. Clicar nessa opção abrirá a janela **Edição de conexão**. Para adicionar uma nova conexão, insira o endereço IP ou o nome do host do servidor, porta a ser usada pela conexão e um comentário (opcional). Clique no botão **Adicionar/Salvar** para adicionar a conexão à lista de servidores no início desta janela. Selecione um servidor específico para mais opções: você pode optar por **Remover**, usar a opção **Remover tudo** ou editar a conexão (semelhante à criação de uma nova conexão).

- **Conectar ao servidor selecionado na inicialização do console** - o console será automaticamente conectado a um ERA Server predefinido.
- **Mostrar mensagem quando a conexão falhar** - se houver um erro de comunicação, um alerta será exibido.

3.5.2 Colunas

Esta guia permite que você especifique quais atributos (colunas) serão exibidos em guias individuais. As alterações serão refletidas no Modo de visualização personalizada (guia Clientes 29). Outros modos não podem ser modificados.

Para exibir uma coluna em uma guia específica, clique no nome da guia na lista de guias e marque as colunas que deseja que sejam exibidas.

- **Selecionar painel** - escolha o painel para o qual deseja alterar a seleção de colunas a serem exibidas.
- **Selecionar colunas a serem exibidas** - selecione as colunas que deseja que sejam exibidas no painel. Escolha cuidadosamente para incluir todas as informações necessárias no painel, mas mantenha a visualização dos dados transparente ao mesmo tempo.
- **Limpar tudo** - desmarca todas as caixas de seleção na janela **Selecionar colunas a serem exibidas** para o painel selecionado.
- **Definir tudo** - marca todas as caixas de seleção na janela **Selecionar colunas a serem exibidas** para o painel selecionado.
- **Padrão** - redefine todas as caixas de seleção na janela **Selecionar colunas a serem exibidas** para padrão para o painel selecionado.
- **Tudo para padrão** - redefine todas as caixas de seleção na janela **Selecionar colunas a serem exibidas** para padrão para todos os painéis.

3.5.3 Cores

Esta guia permite que você associe diferentes cores com eventos específicos relacionados ao sistema, a fim de destacar melhor clientes problemáticos (destaque condicional). Por exemplo, clientes com um banco de dados de assinaturas de vírus ligeiramente desatualizado (**Clientes: Versão anterior**) poderiam ser diferenciados de clientes com um obsoleto (**Clientes: Versões anteriores ou N/D**).

Atribua uma cor específica a painéis e colunas ao selecioná-los na lista **Painel e coluna**. Em seguida, selecione em que cor eles devem ser exibidos.

OBSERVAÇÃO: A cor da coluna **Clientes: Versão anterior ou N/D** será usada quando a versão do Banco de dados de vírus do ESET Smart Security no cliente não for adicionada ou for anterior a do servidor. Ela também será usada quando a versão do produto da ESET Security no servidor for anterior a do cliente ou não adicionada.

Na coluna **Clientes: última conexão**, o intervalo quando usar a coloração poderá ser especificado.

3.5.4 Caminhos

Para acessar configurações do ERA Console, acesse o menu principal do ERAC **Ferramentas** > **Opções do console...**

A guia **Caminhos** permite que você selecione onde seus relatórios gerados pelo ERA Console deverão ser armazenados. Para saber mais sobre como gerar e visualizar relatórios, consulte o capítulo Relatórios 36 deste arquivo de ajuda.

3.5.5 Data/hora

O painel **Data/hora** permite que você personalize opções avançadas para ERA Console. Além disso, aqui você pode selecionar o formato de hora desejado exibido nos registros na janela ERA Console.

- **Absoluto** - o Console exibirá o horário absoluto (p. ex., *"14:30:00"*).
- **Relativo** - o Console exibirá o horário relativo (p. ex., *"há 2 semanas"*).
- **Regional** - o Console exibirá o horário de acordo com configurações regionais (obtidas das configurações do Windows).
- **Recalcular horário UTC para seu horário local (usar horário local)** - marque essa caixa de seleção para recalcular para seu horário local. Caso contrário, será exibido o horário GMT - UTC.

3.5.6 Outras configurações

O painel **Outras configurações** permite que você personalize opções avançadas do ERA Console da ESET.

1. Configurações de filtro

Aplicar alterações automaticamente - se habilitada, os filtros em guias individuais gerarão novas saídas sempre que as configurações de filtro forem modificadas. Caso contrário, o filtro será implementado somente depois de clicar em **Aplicar alterações**.

OBSERVAÇÃO: Se o ERA Console for ser conectado 24 horas por dia, 7 dias da semana, a um ERA Server do PC do administrador, recomenda-se selecionar **Mostrar em barra de tarefas quando minimizado** e deixar o console minimizado quando inativo. Se ocorrer um problema, o ícone systray ficará vermelho - que é um sinal para o administrador intervir. Recomenda-se também ajustar a opção **Usar ícone systray realçado quando clientes problemáticos forem encontrados** - eventos acionando a alteração da cor do ícone.

Atualizações do administrador remoto - esta seção permite que você habilite a verificação para novas versões do ESET Remote Administrator. Recomenda-se o uso do valor padrão (mensal). Se uma nova versão estiver disponível, o ERA Console exibirá uma notificação na inicialização do programa.

2. Outras configurações

- **Usar atualização automática** - atualização automática de dados em guias individuais e no intervalo escolhido.
- **Mostrar linhas de grade** - selecione essa opção para separar células individuais em todas as guias por linhas de grade.
- **Preferir mostrar o Cliente como "Servidor/Nome" em vez de "Servidor/Computador/MAC"** - afeta o modo de exibição para clientes em algumas janelas da caixa de diálogo (por exemplo, **Nova tarefa**). Esta mudança é apenas visual.

- **Usar ícone systray** - o ERA Console será representado por um ícone da bandeja do sistema Windows.
- **Mostrar em barra de tarefas quando minimizado** - se a janela do ERA Console for minimizada, ela estará acessível na barra de tarefas do Windows.
- **Usar ícone systray realçado quando clientes problemáticos forem encontrados** - use essa opção, junto com o botão **Editar** para definir eventos, que acionarão uma alteração da cor do ícone systray.
- **Use hostname no lugar do endereço IP ao executar uma Ação na rede** - Ao executar ações de rede em um cliente (descritas na seção Guia Clientes 29), é possível escolher usar um hostname no lugar de um endereço IP.
- **Mensagens de informações opcionais** - desativa (**Desabilitar tudo**) ou ativa (**Habilitar tudo**) todas as mensagens informativas. Se essa opção estiver habilitada, você verá mensagens azuis sublinhadas no ERA Console. Se você clicar nessas mensagens, elas abrirão dicas e sugestões sobre como sobre usar o produto.

3.6 Modos de exibição

O ERAC oferece ao usuário dois modos de exibição:

- **Modo administrativo** - o modo administrativo do ERAC fornece ao usuário total controle de todos os recursos e configurações, bem como a capacidade de administrar todas as estações de trabalho clientes conectadas a ele.
- **Modo somente leitura** - o modo somente leitura é adequado para visualização do status de soluções clientes da ESET conectando-se ao ERAS; a criação de tarefas para estações de trabalho clientes, a criação de pacotes de instalação e instalação remota não são permitidas. O Gerenciador de licenças, o Gerenciador de políticas e o Gerenciador de notificações também estão inacessíveis. O modo somente leitura permite que o administrador modifique as configurações do ERAC e gere relatórios.

O modo de exibição é selecionado em cada inicialização do console no menu suspenso **Acesso**, enquanto a senha para conectar-se ao ERAS pode ser definida para qualquer modo de exibição. Definir uma senha é especialmente útil se você quiser que alguns usuários recebam acesso total ao ERAS e outros acesso somente leitura. Para definir a senha, clique em **Ferramentas** > **Opções do servidor...** > **Segurança** e clique no botão **Alterar...** ao lado de Senha para console (acesso do administrador) ou (Acesso somente leitura) ou use a ferramenta Gerenciador de usuários 94.

3.7 Editor de configuração da ESET

O Editor de configuração da ESET é um importante componente do ERAC e é usado para diversas finalidades. Algumas das mais importantes são a criação do seguinte:

- Configurações predefinidas para pacotes de instalação
- Configurações enviadas como tarefas ou políticas para clientes
- Um arquivo de configuração geral (.xml)

O Editor de configuração faz parte do ERAC e é representado principalmente pelos arquivos *cfgedit.**.

O Editor de configuração permite que o administrador configure remotamente muitos dos parâmetros disponíveis em qualquer produto de segurança da ESET, especialmente aqueles instalados em estações de trabalho clientes. Ele também permite que o administrador exporte configurações para arquivos .xml, que posteriormente podem ser usadas para várias finalidades, como criar tarefas no ERAC, importar uma configuração localmente no ESET Smart Security, etc.

A estrutura usada pelo Editor de configuração é um modelo *.xml*, que armazena a configuração em uma estrutura do tipo árvore. O modelo é armazenado no arquivo *cfgedit.exe*. É por isso que recomendamos que o ERAS e o ERAC sejam atualizados regularmente.

Aviso: O Editor de configuração permite que você modifique qualquer arquivo *.xml*. Evite modificar ou reescrever o arquivo de origem *cfgedit.xml*.

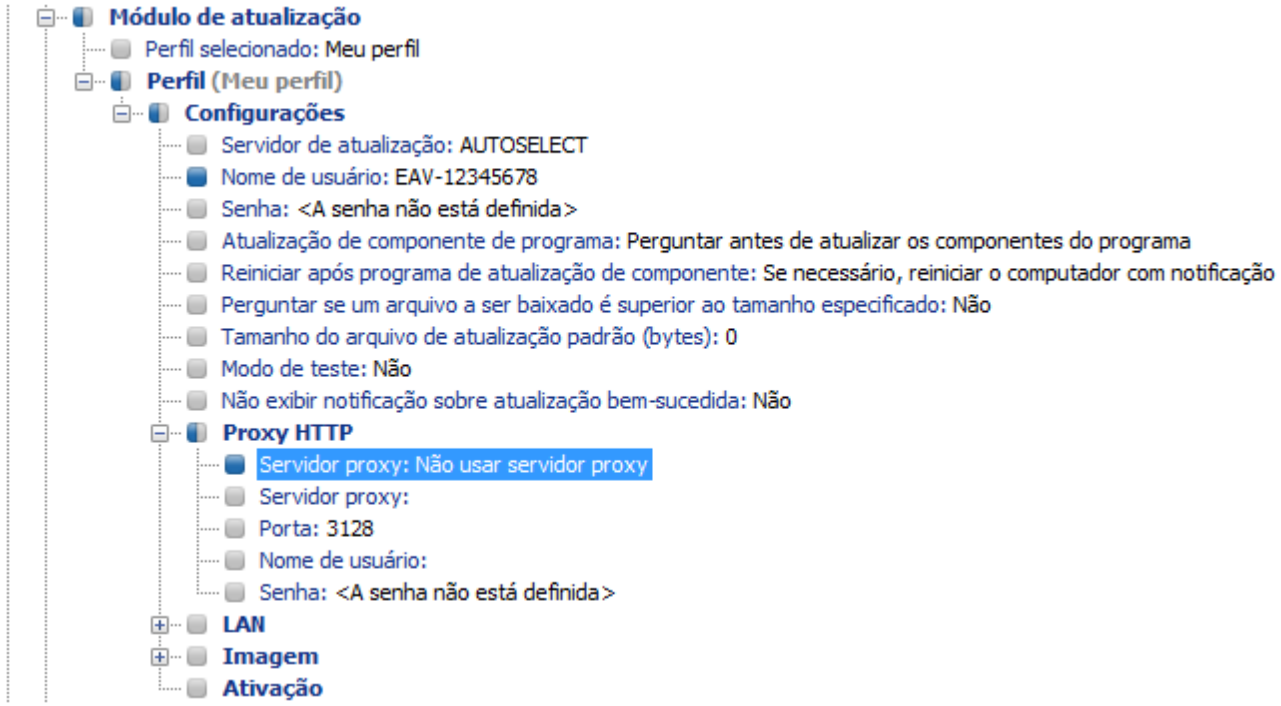
Para que o Editor de configuração funcione, os seguintes arquivos devem estar disponíveis: *eguiHipsRa.dll*, *eguiHipsRaLang.dll*, *eguiRuleManagerRa.dll* e *eset.chm*.

3.7.1 Camadas de configuração

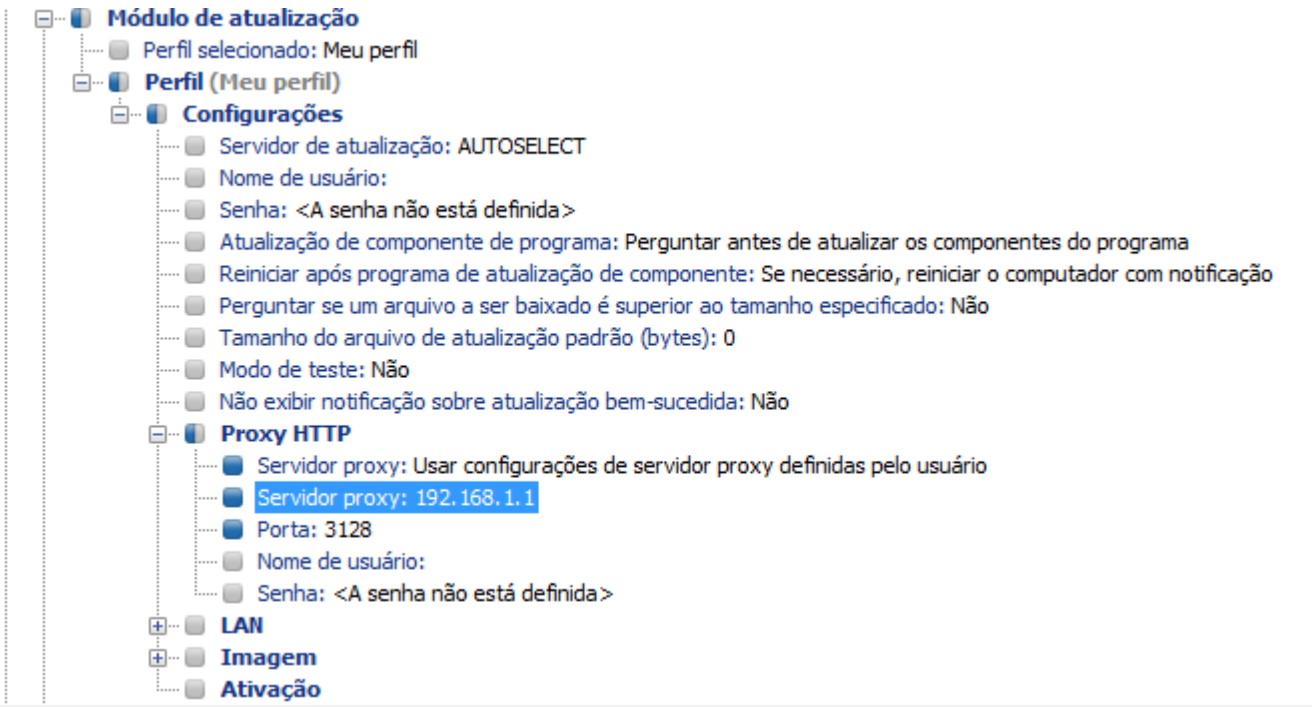
Se um valor for alterado no Editor de configuração, a alteração será marcada por um símbolo azul . Qualquer entrada com o ícone cinza não terá sido alterada e não será gravada na configuração de saída *.xml*.

Ao aplicar uma configuração a clientes, somente modificações que tenham sido salvas no arquivo de configuração de saída *.xml* serão aplicadas (), todos os outros itens () permanecerão inalterados. Esse comportamento permite a aplicação gradual de várias configurações diferentes, sem desfazer modificações anteriores.

Um exemplo é mostrado na figura a seguir. Nesta configuração, o nome de usuário *EAV-12345678* e senha são inseridos e o uso de um servidor proxy é proibido.


Módulo de atualização
Perfil selecionado: Meu perfil
Perfil (Meu perfil)
Configurações
Servidor de atualização: AUTOSELECT
Nome de usuário: EAV-12345678
Senha: <A senha não está definida>
Atualização de componente de programa: Perguntar antes de atualizar os componentes do programa
Reiniciar após programa de atualização de componente: Se necessário, reiniciar o computador com notificação
Perguntar se um arquivo a ser baixado é superior ao tamanho especificado: Não
Tamanho do arquivo de atualização padrão (bytes): 0
Modo de teste: Não
Não exibir notificação sobre atualização bem-sucedida: Não
Proxy HTTP
Servidor proxy: Não usar servidor proxy
Servidor proxy:
Porta: 3128
Nome de usuário:
Senha: <A senha não está definida>
LAN
Imagem
Ativação

A segunda configuração (mostrada na figura a seguir) enviada para os clientes garantirá que as modificações anteriores sejam preservadas, incluindo o nome de usuário *EAV-12345678* e senha. Essa configuração também permitirá o uso de um servidor proxy e definirá seu endereço e porta.


Módulo de atualização
Perfil selecionado: Meu perfil
Perfil (Meu perfil)
Configurações
Servidor de atualização: AUTOSELECT
Nome de usuário:
Senha: <A senha não está definida>
Atualização de componente de programa: Perguntar antes de atualizar os componentes do programa
Reiniciar após programa de atualização de componente: Se necessário, reiniciar o computador com notificação
Perguntar se um arquivo a ser baixado é superior ao tamanho especificado: Não
Tamanho do arquivo de atualização padrão (bytes): 0
Modo de teste: Não
Não exibir notificação sobre atualização bem-sucedida: Não
Proxy HTTP
Servidor proxy: Usar configurações de servidor proxy definidas pelo usuário
Servidor proxy: 192.168.1.1
Porta: 3128
Nome de usuário:
Senha: <A senha não está definida>
LAN
Imagem
Ativação

3.7.2 Principais entradas de configuração

Nesta seção, explicamos várias das principais entradas de configuração para a linha de produto do Windows v3 e v4:

- **Linha de produto do Windows v3 e v4** > **Kernel da ESET** > **Configurações** > **Administração remota**
  Aqui, você pode habilitar a comunicação entre computadores clientes e o ERAS (**Conectar ao Remote Administrator Server**). Insira o nome ou endereço IP do ERAS (**Endereço de servidor primário/secundário**). A opção **Intervalo entre as conexões ao servidor** deve ser deixada no valor padrão de cinco minutos. Para fins de testes, esse valor pode ser diminuído para 0, o que estabelecerá uma conexão a cada dez segundos. Se uma senha for definida, use a que foi especificada no ERAS. Para obter mais informações, consulte a opção **Senha para clientes** no capítulo guia Segurança 93. Informações adicionais sobre a configuração de senha também podem ser encontradas nesta seção.

- **Kernel da ESET** > **Configurações** > **Chaves de licença**
  Os computadores clientes não exigem o acréscimo ou gerenciamento de chaves de licença. As chaves de licença são usadas somente para produtos de servidor.

- **Kernel da ESET** > **Configurações** > **ESET Live Grid**
  Essa ramificação define o comportamento do Sistema de alerta antecipado ESET Live Grid, que permite o envio de arquivos suspeitos para análise aos laboratórios da ESET. Ao implantar soluções da ESET em uma rede grande, as opções **Enviar arquivos suspeitos** e **Ativar o envio de informações estatísticas anônimas** são especialmente importantes: Se elas forem definidas como **Não enviar** ou **Não**, respectivamente, o Sistema ESET Live Grid será totalmente desabilitado. Para enviar arquivos automaticamente sem interação do usuário, selecione **Enviar sem perguntar** e **Sim**, respectivamente. Se um servidor proxy for usado com a conexão de Internet, especifique os parâmetros de conexão em **Kernel da ESET > Configuração > Servidor proxy**.
  Por padrão, os produtos clientes enviam arquivos suspeitos para o ERAS, que os envia para servidores da ESET. Portanto, o servidor proxy deve ser corretamente configurado no ERAS (**Ferramentas > Opções do servidor > Avançadas > Editar configurações avançadas > ERA Server > Configuração > Servidor proxy**).

- **Kernel da ESET** > **Configurações** > **Proteger parâmetros de configuração**
  Permite que o administrador proteja por senha os parâmetros de configuração. Se uma senha for estabelecida, ela será necessária para acessar os parâmetros de configuração em estações de trabalho clientes. No entanto, a senha não afetará quaisquer alterações na configuração feita no ERAC.

- **Kernel da ESET** > **Configurações** > **Agenda/Planejamento**
  Esta chave contém as opções de Agenda/Planejamento, que permitem que o administrador agende varreduras regulares antivírus, etc.

OBSERVAÇÃO: por padrão, todas as soluções de segurança da ESET contêm tarefas predefinidas (incluindo atualização automática regular e verificação automática de arquivos importantes na inicialização). Na maioria dos casos, não deve ser necessário editar ou adicionar novas tarefas.

- **Kernel da ESET** > **Configurações** > **Valores de interface de usuário padrão**
  As configurações em Valores de interface de usuário padrão (ou seja, **Mostrar tela inicial/Não mostrar tela inicial**) aplicam modificações somente nas configurações padrão do cliente. As configurações do cliente poderão então ser gerenciadas por usuário e não poderão ser alteradas remotamente. Para alterar a configuração remotamente, a opção **Suprimir configurações de usuário** deverá ser definida como **Sim**. A opção **Suprimir configurações de usuário** está disponível somente para clientes executando produtos de segurança da ESET 4.0 ou versões posteriores.

- **Módulo**
  Esta ramificação do Editor de configuração permite que você defina como perfis de atualização são aplicados. Normalmente, é necessário apenas modificar o perfil predefinido **Meu perfil** e alterar as configurações de **Servidor de atualização**, **Nome de usuário** e **Senha**. Se o servidor de atualização estiver definido como **Escolher automaticamente**, será feito download de todas as atualizações dos servidores de atualização da ESET. Nesse caso, especifique os parâmetros de **Nome de usuário** e **Senha** que foram fornecidos no momento da compra. Para obter informações sobre como configurar estações de trabalho clientes para receber atualizações de um servidor local (imagem), consulte o capítulo intitulado Servidor de imagem 102. Para obter mais informações sobre como usar a agenda, consulte o capítulo Agenda 135.

OBSERVAÇÃO: em dispositivos portáteis, como notebooks, dois perfis podem ser configurados; um para fornecer atualização do servidor de imagem e outro para fazer download de atualizações diretamente de servidores da ESET. Para obter mais informações, consulte o capítulo Atualização combinada para notebooks 137 no fim deste documento.

4. Instalação de soluções clientes da ESET

Este capítulo é dedicado à instalação das soluções clientes da ESET para sistemas operacionais Microsoft Windows. As instalações podem ser realizadas diretamente 53 em estações de trabalho ou remotamente 44 do ERAS. Este capítulo também descreve métodos alternativos de instalação remota.

OBSERVAÇÃO: Embora seja tecnicamente viável, não recomendamos que o recurso de instalação remota seja usado para instalar produtos da ESET em servidores (somente em estações de trabalho).

Importante: Os administradores, que usam o programa de conexão de área de trabalho remota da Microsoft para acessar computadores clientes remotos, devem ler o artigo a seguir antes de instalar remotamente o ESET Smart Security.

4.1 Instalação direta

Com uma instalação direta, o administrador estará presente no computador no qual o produto de segurança da ESET será instalado. Esse método não requer outra preparação e é adequado para pequenas redes de computador ou em cenários em que o ERA não é usado.

Essa tarefa pode ser muito simplificada com a ajuda de um arquivo de configuração predefinida .xml. Não são necessárias outras modificações, como definir um servidor de atualização (nome de usuário e senha, caminho para um servidor de Imagem, etc.), modo silencioso, rastreamento agendado, etc. durante ou após a instalação.

Há diferenças na aplicação do formato de configuração .xml entre versões 5.x, 4.x, 3.x e 2.x de soluções clientes da ESET:

- Versão 5.x: aplique as mesmas etapas que para a Versão 4.x.

OBSERVAÇÃO: posteriormente, você poderá instalar produtos de segurança da ESET para Linux e Max depois que os clientes v.5 forem lançados.

- Versão 4.x: faça download do arquivo de instalação (p. ex., *ess_nt32_enu.msi*) do*eset.com* e crie seu próprio pacote de instalação no **Editor de pacotes de instalação**. Edite/selecione a configuração que você deseja associar a esse pacote, pressione o botão **Copiar...** ao lado do campo **Pacote para sistemas Windows NT de xx bits** e salve o pacote como **Arquivo Msi de instalação da ESET com configuração (*.msi)**.

  OBSERVAÇÃO: adicionar uma configuração ao arquivo de instalação *.msi* significa que a assinatura digital desse arquivo não será mais válida. Além disso, as etapas da versão 3.x aplicam-se também à versão 4.x.

- Versão 3.x: faça download do arquivo de instalação (p. ex., *ess_nt32_enu.msi*) do *eset.com*. Copie o arquivo de configuração (*cfg.xml*) no diretório no qual o arquivo de instalação está localizado. Após a execução, o instalador adotará automaticamente a configuração do arquivo de configuração *.xml*. Se o arquivo de configuração *.xml* tiver outro nome ou estiver localizado em algum outro local, o parâmetro *ADMINCFG ="path_to_xml_file"* pode ser usado (p. ex., *ess_nt32_enu.msi ADMINCFG ="\\server\xml\settings.xml"* para aplicar a configuração armazenada em uma unidade de rede).

OBSERVAÇÃO: se você estiver instalando o ESET Smart Security (inclui firewall pessoal), será necessário permitir o compartilhamento e a administração remota nessas soluções. Caso contrário, a comunicação de rede entre tais clientes e o ERA Server seria bloqueada.

4.2 Instalação remota

A instalação remota elimina a necessidade de pré-instalação ou instalação física de produtos de segurança em computadores clientes. O ERA oferece vários métodos de instalação remota.

A instalação remota através do ERA consiste nas seguintes etapas:

- Criação de pacotes de instalação

  Primeiro, verifique os requisitos 54 da instalação remota.

  Em seguida, crie pacotes de instalação 44 que sejam distribuídos para os clientes.

- A distribuição de pacotes para estações de trabalho clientes (método de instalação forçada, script de logon, email, atualização, solução externa):

Verifique/configure seu ambiente de rede para instalação remota.

Distribua os pacotes de instalação a clientes. Há vários métodos de instalação remota:

Instalação forçada remota 55. Esse é o método mais eficiente para distribuir produtos de segurança para seus clientes.

Você também pode realizar uma instalação remota por email/logon 57.

Se você não quiser usar os métodos acima, poderá realizar uma instalação remota personalizada 60.

Se alguns clientes tiverem produtos de segurança da ESET anteriores instalados, você poderá atualizá-los para a versão mais recente; consulte o capítulo atualização do cliente 61. Se eles tiverem a versão mais recente, consulte o capítulo evitando instalações repetidas 61. Para instalar pacotes em um ambiente empresarial de grande porte, consulte o capítulo instalação em um ambiente empresarial 62.

4.2.1 Requisitos

A instalação remota requer uma rede TCP/IP corretamente configurada, que fornece comunicação confiável com o servidor cliente. Instalar uma solução cliente usando o ERA impõe condições mais rígidas na estação de trabalho cliente do que uma instalação direta. As seguintes condições devem ser atendidas para instalação remota:

Windows

- Cliente de rede Microsoft habilitado
- Serviço de compartilhamento de arquivos e impressoras habilitado
- As portas de compartilhamento de arquivos (445, 135 - 139) estão acessíveis
- Protocolo TCP/IP
- Compartilhamento administrativo ADMIN$ habilitado
- O cliente pode responder a solicitações PING
- Conectividade do ERAS e ERAC (as portas 2221- 2224 estão acessíveis)
- Já existe nome de usuário e senha de administrador para estações de trabalho clientes (o nome de usuário não de ser deixado em branco)
- Compartilhamento simples de arquivos desabilitado
- Serviço de servidor habilitado
- Serviço de registro remoto habilitado

OBSERVAÇÃO: versões recentes do Microsoft Windows (Windows Vista, Windows Server 2008 e Windows 7) aplicam políticas de segurança limitando permissões de conta de usuário local, de forma que o usuário talvez não consiga executar operações de rede específicas. Se o seu serviço ERA estiver em execução em uma conta de usuário local, problemas de instalação forçada poderão ocorrer em determinadas configurações específicas de rede (p. ex., ao instalar remotamente de um domínio para um grupo de trabalho). Ao usar o Windows Vista, Windows Server 2008 ou Windows 7, recomendamos o uso do serviço ERA em contas com direitos de rede suficientes. Para especificar a conta de usuário na qual deseja executar o ERA, acesse **Iniciar** ? **Painel de controle** → **Ferramentas administrativas** → **Serviços**. Selecione o serviço ESET Remote Administrator Server da lista e clique em **Fazer logon**. O ESET Remote Administrator 5 incorpora essa configuração no cenário de instalação avançada; portanto, você deve selecionar **Avançado** ? **Instalação totalmente personalizada** durante a instalação.

Importante: Se você estiver usando a **Instalação forçada** em estações de trabalho com Windows Vista, Windows Server 2008 ou Windows 7, certifique-se de que seu ERA Server, bem como as estações de trabalho de destino estejam em um domínio.

Além disso, recomendamos que o administrador desative o UAC (User Access Control, Controle de acesso para usuário) para Windows Vista, Windows 7 e Windows Server 2008. Isso pode ser feito clicando em **Iniciar** > **Painel de controle** > **Contas de usuário** > **Ativar ou desativar controle de conta de usuário** ou pode clicar em **Iniciar** >, insira**Msconfig** no campo de pesquisa e pressione **Inserir** > **Ferramentas** > **Desativar UAC (requer reinicialização)**.

Recomendamos extremamente que você verifique todos os requisitos antes da instalação, especialmente se houver várias estações de trabalho na rede (na guia **Instalação remota**, selecione a guia **Computadores**, clique com o botão direito do mouse nos clientes relevantes e selecione **Diagnóstico de instalação forçada** no menu de contexto).

Importante: os administradores, que usam o programa de conexão de área de trabalho remota da Microsoft para acessar computadores clientes remotos, devem ler o artigo a seguir antes de instalar remotamente o ESET Smart Security.

4.2.1.1 Requisitos para instalação forçada de Linux/Mac

Certifique-se de que todas as estações de trabalho do cliente estão configuradas corretamente antes de realizar uma instalação remota.

- **Linux**

1. O computador deve ser capaz de se conectar ao servidor via SSH.
2. A conta SSH deve ter direitos de administrador - isso significa que você precisa executar a instalação no usuário raiz (UID=0) ou um usuário que tenha direitos de sudo.

- **Mac**

1. O computador deve ser capaz de se conectar ao servidor via SSH.
2. A conta SSH deve ter direitos de administrador - isso significa que você precisa executar a instalação em um usuário que seja um administrador.

Observação: Este recurso é compatível com o ESET NOD32 Antivirus Business Edition for Mac OS X 4.1.94 e ESET NOD32 Antivirus Business Edition for Linux Desktop 4.0.79 e todas as versões posteriores para ambas as plataformas.

4.2.2 Instalação forçada remota

O método de instalação remota força soluções clientes da ESET em computadores remotos. A instalação forçada é o método de instalação mais eficaz, bem como requer que todas as estações de trabalho de destino estejam on-line. Antes de iniciar uma instalação forçada, faça download dos arquivos de instalação .msi para ESET Smart Security ou ESET NOD32 Antivirus do site da ESET e crie um pacote de instalação. Você pode criar um arquivo de configuração .xml que será automaticamente aplicado quando o pacote for executado. Consulte o capítulo sobre Requisitos 54 antes da instalação.

Para iniciar uma instalação forçada, siga estas etapas:

1) Assim que os computadores adequados para instalação forçada forem relacionados na guia **Computadores**, você poderá selecionar todos ou alguns deles e executar uma tarefa de instalação forçada clicando com o botão direito do mouse na janela e selecionando **Instalação forçada** no menu de contexto.

2) Defina as informações de logon para computadores na lista (**Definir**, **Definir tudo**). Isso deve ser feito usando uma conta com direitos de administrador. Você ainda pode adicionar clientes à lista nessa etapa usando o recurso Especial **Adicionar clientes**.

3) Selecione o pacote de instalação 44 desejado a ser fornecido para estações de trabalho clientes.

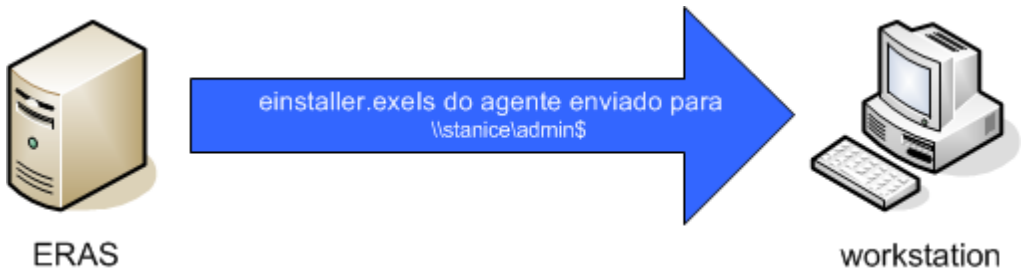
4) Defina o horário quando a tarefa deve ser executada e clique em **Concluir**.

Você pode visualizar o status da tarefa de instalação forçada na guia Tarefas de instalação 47. Para obter detalhes de resultados diagnósticos, selecione a tarefa desejada e pressione F4. A janela **Propriedades** será exibida na guia **Detalhes**, na qual você poderá visualizar resultados diagnósticos da instalação remota clicando em **Exibir todos os logs/Exibir logs selecionados**.

OBSERVAÇÃO: o número máximo de ameaças simultâneas de instalação forçada será definido como 20 por padrão. Se você enviar uma tarefa de instalação forçada para vários computadores excedendo esse limite, os computadores adicionais serão colocados na fila e aguardarão até que as ameaças estejam resolvidas. Não recomendamos aumentar esse valor por motivos de desempenho; no entanto, se você considerá-lo necessário, poderá alterar o limite no Editor de configuração (**ESET Remote Administrator** > **ERA Server** > **Configuração** > **Instalação remota**).

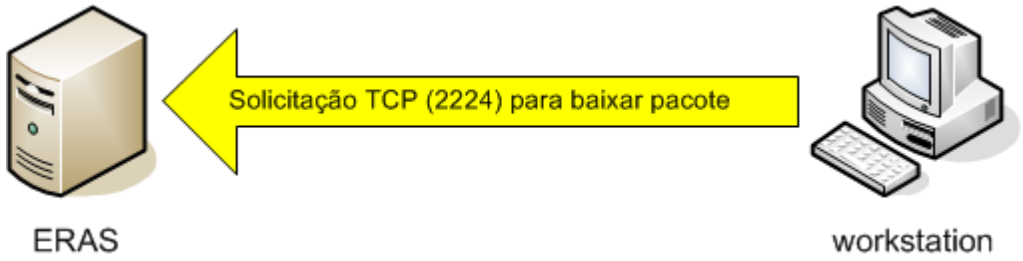
Os detalhes do processo de instalação remota são descritos a seguir:

5) O ERAS envia o agente *einstaller.exe* para a estação de trabalho com a ajuda do compartilhamento administrativo admin$.

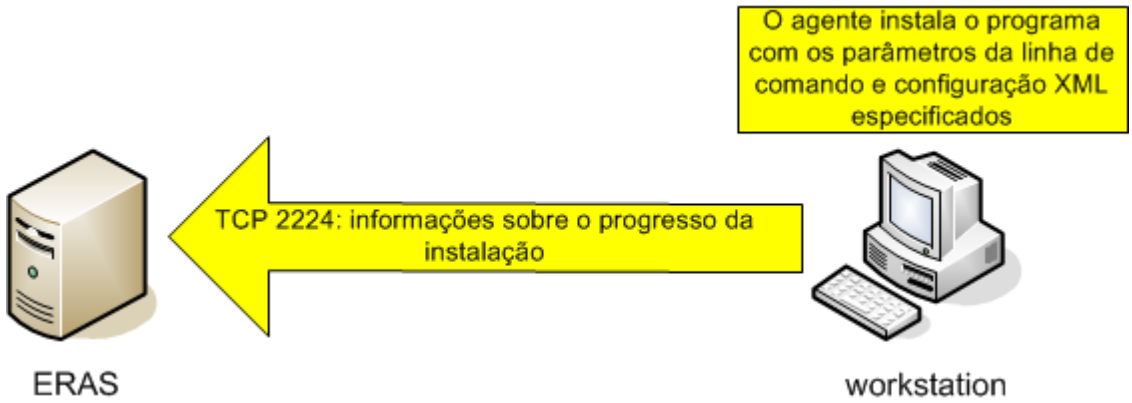


6) O agente inicia como um serviço na conta do sistema.

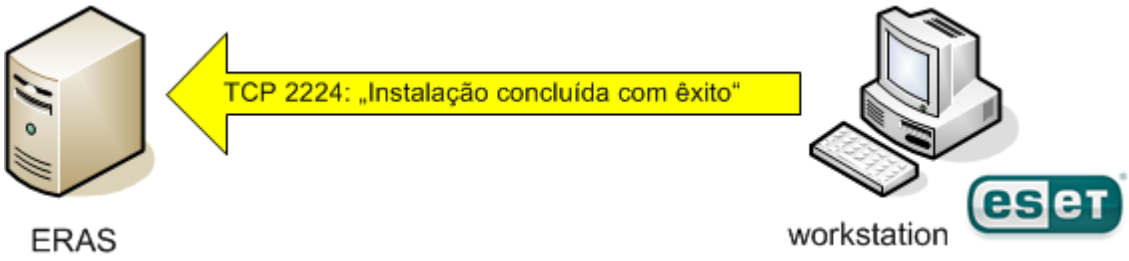
7) O agente estabelece comunicação com seu ERAS "pai" e faz download do pacote de instalação correspondente na porta TCP 2224.



8) O agente instala o pacote na conta do administrador definido na etapa 2; os parâmetros da linha de comando e configuração *.xml* correspondentes também são aplicados.


O agente instala o programa com os parâmetros da linha de comando e configuração XML especificados
TCP 2224: informações sobre o progresso da instalação
ERAS
workstation

9) Imediatamente depois que a instalação for concluída, o agente enviará uma mensagem de volta para o ERAS. Alguns produtos de segurança da ESET exigem uma reinicialização e avisarão você, se necessário.



4.2.3 Instalação remota por logon/email

Os métodos de instalação remota por logon e email são muito semelhantes. Eles variam somente na forma como o agente *einstaller.exe* é fornecido a estações de trabalho clientes. O ERA permite que o agente seja executado por script de logon ou por email. O agente *einstaller.exe* também pode ser usado individualmente e executado através de outros métodos (para obter mais informações, consulte o capítulo Instalação remota personalizada 60).

O método de logon funciona bem para notebooks que são usados frequentemente fora da rede local. A instalação será realizada depois do logon no domínio.

Enquanto o script de logon é executado automaticamente quando o usuário efetua logon, o método de email requer a intervenção por parte do usuário, que deverá iniciar o agente einstaller.exe a partir de um anexo de email. Se iniciado separadamente, o installer.exe não acionará outra instalação de soluções clientes da ESET. Para obter mais informações, consulte o capítulo Evitando instalações repetidas 61.

Para obter um guia detalhado sobre como exportar o ESET Installer para a pasta/script de logon, consulte este capítulo 58.

Enviar instalador da ESET por email

Primeiro selecione o tipo de ESET Installer.

- **Produtos de segurança da ESET para Windows**

1. Selecione um pacote criado anteriormente no menu suspenso **Pacote**.
2. Digite o endereço de email do destinatário no campo **Para**.
3. Opcionalmente, é possível editar o **Assunto** e **Descrição** do email e clicar em **Enviar** para enviar o agente *einstaller.exe* para o usuário.

- **Desinstalar produtos de segurança da ESET para Windows e NOD32 versão 2**

Usando este tipo, é possível desinstalar todos os produtos de segurança ESET do computador do usuário.

- **Produtos de segurança da ESET para Android**

Importante: Antes de prosseguir, leia este capítulo 76.

1. Clique em **...** perto do campo **Anexo** e navegue até o local onde você salvou seu produto de segurança ESET para Android (arquivo *.apk*). Selecione este aplicativo e clique em **OK**.
2. Digite o email do usuário, revise ou edite as informações nos campos **Assunto** e **Descrição** e clique em **...** ao lado do link de configuração. Isto vai abrir a janela de **Definição das configurações de link**, onde você pode configurar a forma como o produto se conecta ao ERA.

Observação: Este link vai configurar o produto de segurança ESET para Android que precisa ser instalado (é possível enviar um link com o arquivo de instalação para o usuário, ou enviar o aplicativo diretamente, conforme descrito na Etapa 1).

3. Os campos **Servidor** e **Porta** são pré-definidos com base em seu ERA Server atual. Se for necessária uma senha para que os usuários se conectem ao servidor, digite-a no campo **Senha**. Caso contrário, deixe este campo em branco. Se usar uma senha, a opção **Adicionar o SIM atual como confiável** deve ser selecionada. Ela é selecionada por padrão para evitar que o celular seja bloqueado ao tentar conectar-se ao ERA Server. Estas configurações básicas serão enviadas ao cliente. Para configurações avançadas (como atualizar o **Nome de usuário** e **Senha**), o cliente precisa estar conectado ao ERA Server e você pode distribuir essas configurações usando uma Política 71.

- **Personalizar pacote**

Você pode enviar um pacote de instalação personalizado (descrito aqui 44) para um usuário selecionado.

4.2.3.1 Exportar instalador da ESET para pasta/script de logon

Você pode usar um editor de texto ou outra ferramenta proprietária para inserir a linha chamando *einstaller.exe* no script de logon. Da mesma forma, o *einstaller.exe* pode ser enviado como um anexo de email usando o cliente de email. Independentemente do método usado, certifique-se de que você esteja usando o arquivo *einstaller.exe* correto.

Para que o *einstaller.exe* inicie, o usuário atualmente conectado não precisa necessariamente ser um administrador. O agente adota o nome de usuário/senha/domínio do administrador necessário do ERAS. Para obter mais informações, consulte o final deste capítulo.

Insira o caminho para *einstaller.exe* no script de logon:

1) Clique com o botão direito do mouse em uma entrada na guia **Instalação remota**, clique em **Exportar para pasta ou script de logon**, e selecione o **Tipo** e o nome do **Pacote** a ser instalado.

2) Clique em **...** ao lado de **Pasta** para selecionar o diretório no qual o arquivo *einstaller.exe* está localizado e disponível na rede, e então clique em **OK**.

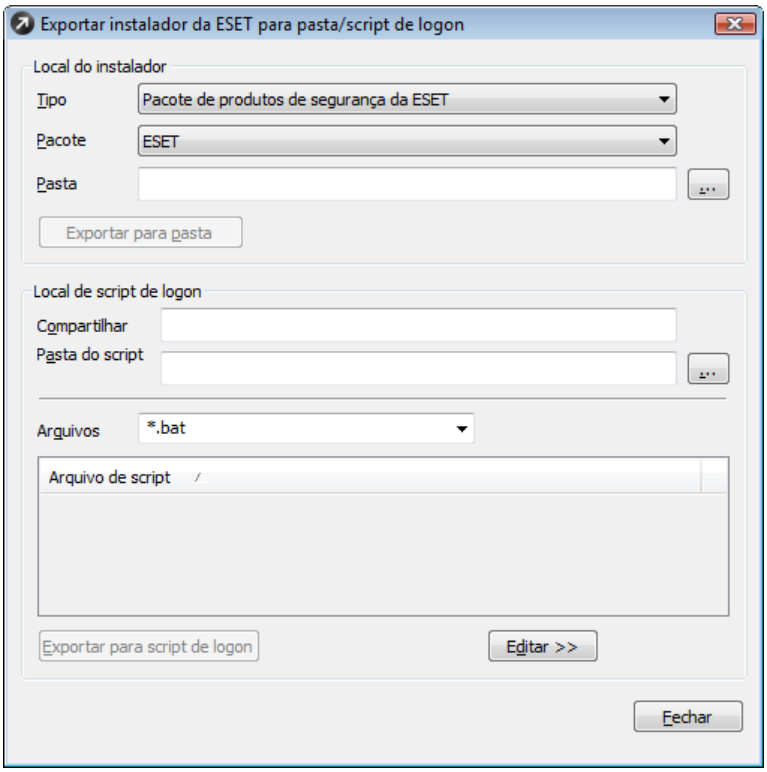
3) No campo **Compartilhar**, certifique-se de que o caminho esteja correto ou edite-o, se necessário.

4) Clique em **...** ao lado de **Pasta do script** para selecionar a pasta na qual o script está localizado e modifique a máscara, se necessário (**Arquivos**).

5) Na seção **Arquivos**, selecione o arquivo no qual a linha chamando o *einstaller.exe* será inserida.

6) Clique em **Exportar para script de logon** para inserir a linha.

7) A localização da linha pode ser modificada clicando-se em **Editar >>** e salva clicando-se em **Salvar**.



Anexando o agente (*einstaller.exe*) ao email:

1) Clique em **Email...** na guia **Instalação remota** e selecione o **Tipo** e nome do **Pacote** que deseja instalar.

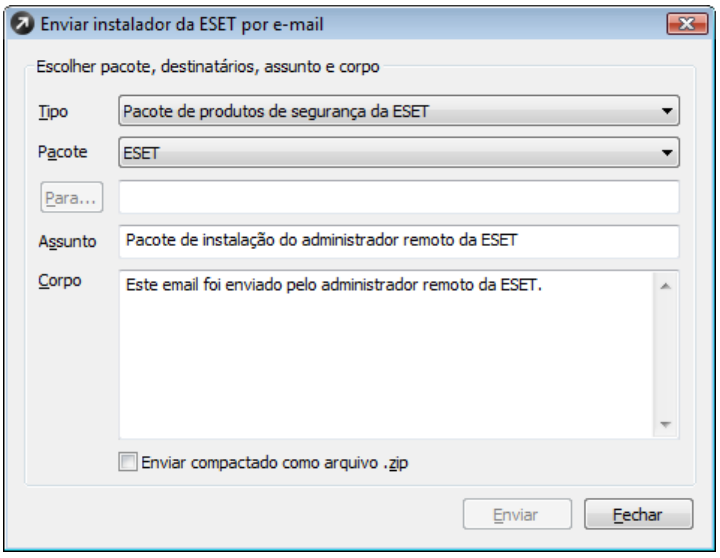
2) Clique em **Para...** para selecionar endereços do catálogo de endereços (ou insira endereços individuais).

3) Insira um **Assunto** no campo correspondente.

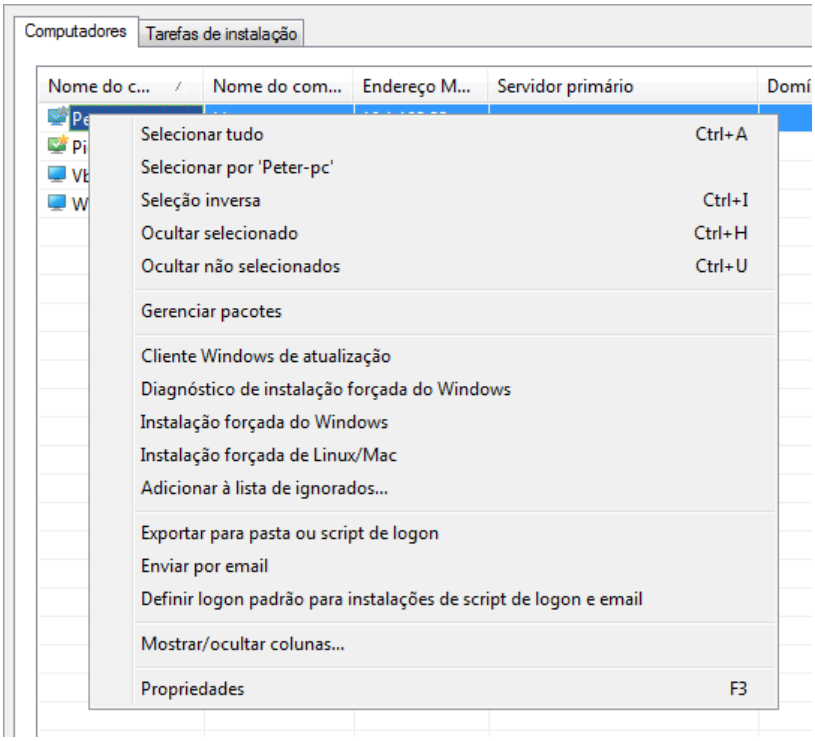
4) Insira uma mensagem no **Corpo**.

5) Marque a caixa de seleção ao lado de **Enviar compactado como arquivo .zip** se quiser enviar o agente como um pacote compactado.

6) Clique em **Enviar** para enviar a mensagem.



Durante o processo de instalação remota, a conexão reversa para o ERAS ocorrerá e o agente (*einstaller.exe*) adotará as configurações da opção Definir logon padrão para instalações de script de logon e email no menu de contexto.



A conta na qual a instalação do pacote será realizada deve ser de uma conta com direitos de administrador ou, de preferência, uma conta do administrador do domínio. Os valores inseridos na janela da caixa de diálogo **Logon padrão...** serão esquecidos depois de cada reinicialização do serviço (ERAS).

4.2.3.2 Logon padrão

A janela **Logon padrão** permite que você defina as credenciais de usuário e informações de domínio necessárias para acessar seu computador cliente na rede, bem como gerenciar o produto da ESET instalado.

Os dados de cliente necessários são:

- **Nome de usuário**
- **Senha**
- **Domínio/grupo de trabalho**

Depois de inserir os dados, pressione o botão **Definir logon** para salvar as informações no servidor.

OBSERVAÇÃO: observe que essas informações serão armazenadas somente no servidor até a próxima reinicialização do servidor.

OBSERVAÇÃO: se você vir a mensagem *The logon information is already stored on the server* (As informações de logon já estão armazenadas no servidor), na janela **Logon padrão**, as configurações já foram armazenadas no servidor. Se você quiser alterar as configurações armazenadas, clique no botão **Substituir** e continue configurando as novas informações de logon.

4.2.4 Instalação remota personalizada

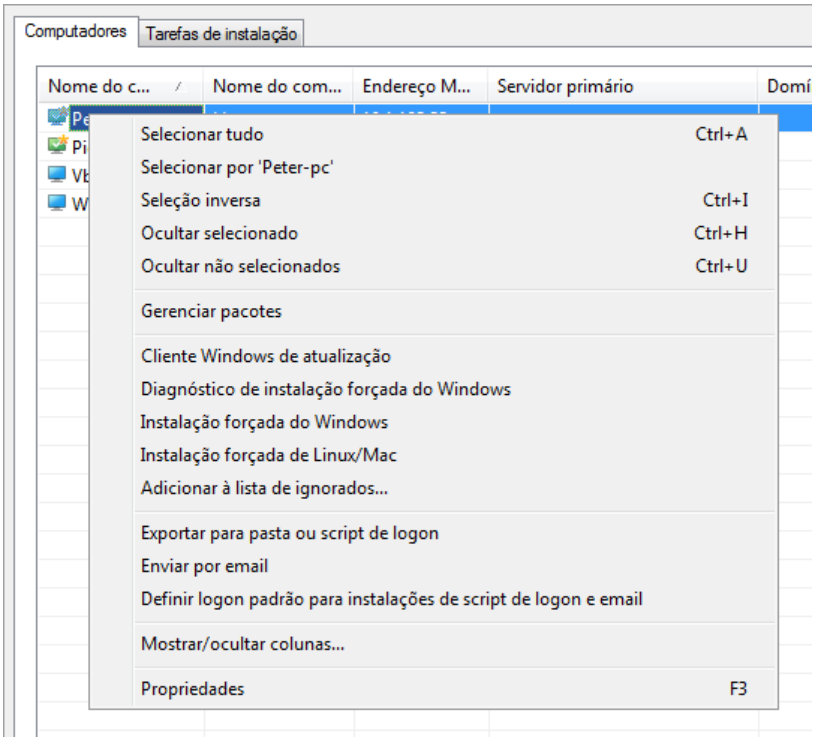
Não é um requisito usar ferramentas do ERA para instalar remotamente soluções clientes da ESET. Por fim, o aspecto mais importante é fornecer e executar o arquivo *einstaller.exe* em estações de trabalho clientes.

Para que o *einstaller.exe* inicie, o usuário atualmente conectado não precisa necessariamente ser um administrador. O agente adota o nome de usuário/senha/domínio do administrador necessário do ERAS. Para obter mais informações, consulte o final deste capítulo.

O arquivo *einstaller.exe* pode ser obtido da seguinte forma:

- Na guia **Computadores** (na guia **Instalação remota**), clique com o botão direito do mouse em qualquer parte e selecione **Exportar para pasta ou script de logon** no menu de contexto. Selecione o **Tipo** e insira o nome do **Pacote** a ser instalado.
- Clique no botão **...** ao lado de **Pasta** e selecione o diretório no qual o *einstaller.exe* será exportado.
- Clique no botão **Exportar para pasta**.
- Use o arquivo *einstaller.exe* extraído.

OBSERVAÇÃO: o método *"Instalação direta com configuração XML predefinida"* pode ser usado em situações nas quais é possível fornecer direitos de administrador para a instalação. O pacote *.msi* é iniciado usando o parâmetro */qn* (versões 5.x, 4.x, 3.x). Esses parâmetros executarão a instalação sem exibir uma interface do usuário.



O nome de usuário e senha da conta na qual a instalação do pacote será realizada devem ser de uma conta com direitos de administrador ou, de preferência, uma conta do administrador do domínio.

Durante o processo de instalação remota, a conexão retrógrada para o ERAS ocorrerá e o agente (*einstaller.exe*) adotará as configurações da opção **Definir logon padrão para instalações de script de logon e email**.

Se o agente *einstaller.exe* for iniciado manualmente em uma estação de trabalho de destino, a instalação remota será processada da seguinte forma:

- O agente *einstaller.exe* envia uma solicitação para o ERAS (porta TCP 2224).
- O ERAS inicia uma nova instalação forçada (com um novo agente) do pacote correspondente (enviada através do compartilhamento *admin$*). O agente aguarda uma resposta do ERAS (enviando o pacote através do compartilhamento *admin$*). Na hipótese de que nenhuma resposta ser recebida, o agente tentará fazer download do

pacote de instalação (através da porta TCP/IP 2224). Nesse caso, o nome de usuário e senha do administrador especificados em **Instalação remota > Logon...** no ERAS não serão transferidos e o agente tentará instalar o pacote no usuário atual. Nos sistemas operacionais Microsoft Windows 9x/Me, o compartilhamento administrativo não pode ser usado; portanto, o agente estabelece automaticamente uma conexão TCP/IP direta com o servidor. O novo agente então começa a fazer o download do pacote do ERAS através do protocolo TCP/IP.

A instalação do pacote é iniciada, aplicando-se os parâmetros .xml associados na conta definida no ERAS (a opção **Definir logon padrão para instalações de script de logon e email**).

4.2.5 Cliente de atualização

Este tipo de instalação foi desenvolvido para clientes com o ESS/EAV versão 4.2 e posteriores. A partir da versão 4.2, um novo mecanismo de atualização foi implementado, permitindo que o ERA inicie o processo de atualização por parte do cliente, sem a necessidade do agente *einstaller.exe*. Esse mecanismo funciona de forma semelhante à atualização de componente do programa, ou PCU (Program Component Update), que atualiza clientes para uma versão mais recente do programa. Para a versão 4.2 e clientes ESS/EAV posteriores, recomendamos extremamente esse tipo de atualização.

OBSERVAÇÃO: se um arquivo de configuração personalizada tiver sido definido para o pacote de instalação, ele será ignorado durante a atualização.

O comando **Cliente de atualização** permite que você atualize remotamente um cliente/grupo de clientes.

1) Clique no botão **Adicionar especial de clientes** na primeira etapa se você quiser usar a ferramenta de seleção para escolher quais clientes atualizar. Depois de concluir suas seleções, clique em **Avançar** para continuar.

OBSERVAÇÃO: clicar em **Adicionar especial de clientes** abrirá uma nova janela na qual você pode adicionar clientes por servidor (na seção **Servidores**) ou por grupo (na seção **Grupos**).

2) Na janela **Configurações de pacote**, você pode usar os respectivos menus suspensos para selecionar o **Tipo** e o **Nome** de um pacote de produto da ESET que será usado para atualizar seus clientes. Depois de concluir suas seleções, clique em **Avançar** para continuar.

3) Na janela **Configurações de tarefa**, você pode alterar o nome padrão e descrição de sua tarefa de atualização, selecionar **Aplicar tarefa** agora se quiser que a tarefa seja executada imediatamente ou **Aplicar tarefa posteriormente** se você quiser configurar uma data posterior para a execução da tarefa. Clique em **Concluir** para concluir a configuração de sua tarefa do cliente de atualização.

OBSERVAÇÃO: essa tarefa funciona somente em clientes que se conectam diretamente ao servidor primário. clientes de servidores replicados serão ignorados.

4.2.6 Evitando instalações repetidas

Imediatamente depois de o agente concluir com êxito o processo de instalação remota, ele marcará o cliente remoto com um sinalizador, proibindo instalações repetidas do mesmo pacote de instalação. O sinalizador é gravado na seguinte chave de registro:

HKEY_LOCAL_MACHINE\Software\ESET\ESET Remote Installer

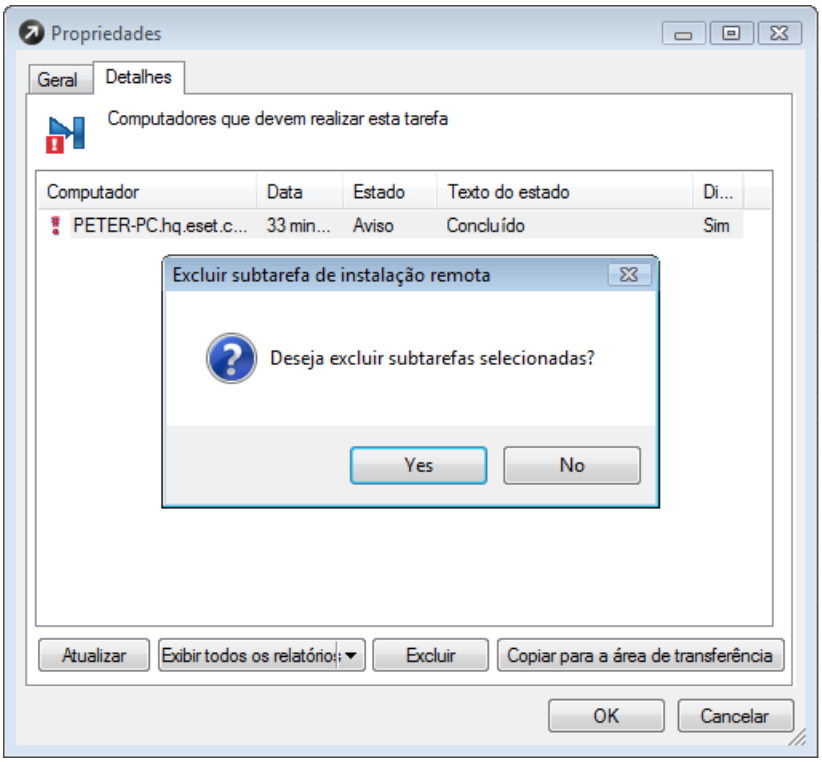
Se o Tipo e Nome do pacote definido no agente *einstaller.exe* corresponderem aos dados no registro, a instalação não será realizada. Isso impede que instalações repetidas tenham como alvo as mesmas estações de trabalho.

OBSERVAÇÃO: o método de instalação forçada remota ignora essa chave de registro.

O ERAS fornece um recurso adicional para impedir que instalações repetidas sejam ativadas quando o instalador estabelecer conexão retrógrada com o ERAS (TCP 2224). Se houver uma mensagem de erro relacionada à estação de trabalho ou a instalação tiver sido concluída com êxito, quaisquer tentativas adicionais de instalação serão negadas.

O agente registra o seguinte erro no log do instalador, localizado em *%TEMP%\einstaller.log*:

O ESET Installer foi instruído a sair pelo servidor 'X:2224'.



Para impedir que instalações repetidas sejam negadas pelo ERAS, as entradas relacionadas na guia **Detalhes da Tarefa de instalação remota** deverão ser removidas. Para excluir qualquer entrada, selecione-a, clique no botão **Excluir** e confirme pressionando **Sim**.

4.3 Instalação em um ambiente empresarial

Ao implantar programas em grandes redes, é importante usar uma ferramenta com capacidade para realizar instalações de programa remoto em cada e todos os computadores na rede.

Instalando usando uma política de grupo

No ambiente Active Directory, essa tarefa pode ser resolvida com facilidade por uma instalação de política de grupo. A instalação usa o instalador MSI, que é distribuído diretamente para todos os clientes conectando-se ao domínio através da política de grupo.

Para configurar um controlador de domínio para instalar automaticamente o ESET Smart Security ou o ESET NOD32 Antivirus em cada estação de trabalho depois de fazer login, proceda da seguinte forma:

1) Crie uma pasta compartilhada no controlador do seu domínio. Todas as estações de trabalho devem ter permissão de "leitura" para essa pasta.

2) Copie o pacote de instalação do ESET Smart Security ou ESET NOD32 Antivirus (*.msi*) para a pasta.

3) Insira um arquivo de configuração *.xml*, que é aplicado no programa, na mesma pasta. O arquivo deve ser nomeado *cfg.xml*. Para criar um arquivo de configuração, o Editor de configuração da ESET poderá ser usado. Para obter mais informações, consulte o capítulo Editor de configuração da ESET 50.

4) Clique em **Iniciar** > **Programas** > **Ferramentas administrativas** > **Usuários e computadores do Active Directory**.

5) Clique com o botão direito do mouse no nome de domínio e selecione **Propriedades** > **Política de grupo** > **Editar** > **Configuração do usuário**.

6) Clique com o botão direito do mouse em **Configurações de software** e selecione **Novo** > **Pacote**.

7) Na janela **Abrir**, especifique o caminho de UNC para o pacote de instalação compartilhada, ou seja, \ *computer_name**path**installation_package.msi* e clique em **Abrir**. Não use a opção **Procurar** para localizar o pacote de instalação, pois ele será exibido como um caminho de rede local em vez de um caminho de rede UNC.

8) Na próxima janela da caixa de diálogo, selecione a opção **Atribuído**. Em seguida, clique em **OK** para fechar a janela.

Ao seguir as etapas acima, o pacote do instalador será instalado em cada computador que entrar no domínio. Para instalar o pacote em computadores que estão atualmente em execução, esses usuários devem fazer logout e fazer login novamente.

Se você quiser fornecer aos usuários a capacidade de aceitar ou negar a instalação do pacote, selecione **Publicar** em vez de **Atribuído** na etapa 8. Na próxima vez que o usuário fizer login, o pacote será adicionado ao **Painel de controle** > **Adicionar ou remover programas** > **Adicionar novo programa** > **Adicionar programas de sua rede**. O pacote então estará disponível para usuários para instalações futuras desse local.

5. Administrando computadores clientes

5.1 Tarefas

As estações de trabalho clientes que forem corretamente conectadas ao ERAS e exibidas no ERAC poderão ser configuradas e administradas usando vários tipos de tarefas.

Fase I - **Nova tarefa**.

1) Para aplicar uma tarefa a uma ou mais estações de trabalho clientes, selecione e clique com o botão direito do mouse nas estações de trabalho no painel **Clientes** para abrir o menu Contexto 27.

2) Clique em **Nova tarefa** e selecione o tipo de tarefa que deseja realizar.

OBSERVAÇÃO: como alternativa, o assistente de tarefa poderá ser aberto do menu principal do ERAC clicando-se em **Ações > Nova tarefa**.

Fase II - selecione uma das seguintes tarefas:

- Tarefa de configuração 65
- Rastreamento sob demanda (limpeza desabilitada/limpeza habilitada) 65
- Atualizar agora 66
- Tarefa de script do SysInspector 66
- Recursos de proteção 66
- Executar tarefa agendada 67
- Restaurar/excluir da tarefa de quarentena 67
- Reversão de banco de dados de vírus 67
- Limpar cache de atualização do cliente 68
- Gerar log de auditoria de segurança 68
- Mostrar notificação 68

3) Depois de escolher a tarefa desejada, você precisará realizar as ações específicas de tarefa descritas em cada um dos capítulos (veja os links acima).

Fase III - **Selecionar clientes**.

4) Você pode modificar suas seleções de cliente na janela **Selecionar clientes**, que serão exibidas assim que você tiver configurado a tarefa. Você poderá refinar sua seleção de cliente ao adicionar clientes da árvore de visão geral de cliente **Todos os itens** (metade esquerda da janela) para a lista **Itens selecionados** (metade direita da janela) ou ao remover as entradas de cliente que já estão na lista.

   OBSERVAÇÃO: clique em **Adicionar especial...** para abrir uma nova janela na qual você pode adicionar clientes do painel **Clientes** ou adicionar clientes pelo **Servidor** e/ou **Grupos**.

Fase IV - concluindo a tarefa 68.

Os subcapítulos seguintes descrevem os tipos individuais de tarefas para estações de trabalho clientes, com um cenário de exemplo acompanhando para cada tipo de tarefa.

OBSERVAÇÃO: a janela **Verificação de atualização do ERA** será exibida quando o intervalo de tempo especificado for decorrido ou quando uma nova versão do produto estiver disponível. Para baixar a atualização do produto mais recente do site da ESET, clique em **Visitar site de atualização**.

5.1.1 Tarefa de configuração

As tarefas de configuração são usadas para modificar configurações de proteção em estações de trabalho clientes. Essas tarefas são fornecidas em estações de trabalho clientes em pacotes de configuração contendo os parâmetros de modificação. Os arquivos *.xml* criados no Editor de configuração da ESET ou exportados de clientes também são compatíveis com tarefas de configuração. O exemplo a seguir demonstra como criar uma tarefa de configuração que altera o nome de usuário e senha em computadores de destino. Quaisquer chaves e opções não usadas neste exemplo serão fornecidas no fim deste capítulo.

Primeiro, designe as estações de trabalho nas quais a tarefa será entregue. Marque essas estações de trabalho no painel **Clientes** no ERAC.

1) Clique com o botão direito do mouse em qualquer uma das estações de trabalho selecionadas e selecione **Nova tarefa** > **Tarefa de configuração** no menu de contexto.

2) A janela **Configuração para clientes** será aberta, que servirá como um assistente de tarefa de configuração. Você pode especificar a origem do arquivo de configuração clicando em **Criar...**, **Selecionar...** ou **Criar de modelo...**

3) Clique no botão **Criar** para abrir o Editor de configuração da ESET e especificar a configuração a ser aplicada. Acesse a **Linha de produto do Windows v3 e v4** > **Módulo de atualização** > **Perfil** > **Configurações** > **Nome de usuário** e **Senha**.

4) Insira o nome de usuário e senha fornecidos pela ESET, e clique em **Console** à direita para retornar ao assistente de tarefa. O caminho para o pacote será exibido no campo **Criar/selecionar configuração**.

5) Se você já tiver um arquivo de configuração que contém as modificações desejadas, clique em **Selecionar**, localize o arquivo e o atribua à tarefa de configuração.

6) Como alternativa, você pode clicar em **Criar de modelo**, selecione o arquivo *.xml* e faça as alterações, se necessário.

7) Para visualizar ou editar o arquivo de configuração que você acabou de criar ou editar, clique nos botões **Visualizar** ou **Editar**.

8) Clique em **Avançar** para prosseguir para a janela **Selecionar clientes**, que mostra as estações de trabalho para as quais a tarefa será entregue. Nessa etapa, você pode adicionar clientes de Grupos ou Servidores selecionados. Clique em**Avançar** para prosseguir até a próxima etapa.

9) A última janela da caixa de diálogo, **Relatório de tarefa**, mostra uma visualização da tarefa de configuração. Insira um nome ou descrição da tarefa (opcional). A opção **Aplicar tarefa após** poderá ser usada para definir a tarefa para execução depois de uma data/hora especificada. A opção **Excluir tarefas automaticamente por limpeza se concluídas com êxito** exclui todas as tarefas que foram entregues com êxito para as estações de trabalho clientes.

10) Clique em **Concluir** para registrar a tarefa para execução.

5.1.2 Tarefa de rastreamento sob demanda

A opção do menu de contexto **Nova tarefa** contém duas variantes do rastreamento sob demanda. A primeira opção é **Rastreamento sob demanda (limpeza desabilitada)** - esse rastreamento apenas cria um log, nenhuma ação será realizada nos arquivos infectados. A segunda opção é **Rastreamento sob demanda (limpeza habilitada)**.

A janela **Rastreamento sob demanda** contém as mesmas configurações padrão para ambas as variantes, além da opção **Rastrear sem limpar**. Essa opção determina se o scanner deve ou não limpar arquivos infectados. O exemplo a seguir demonstra como criar uma tarefa de rastreamento sob demanda.

1) O menu suspenso **Seção de configuração** permite que você selecione o tipo de produto da ESET para o qual a tarefa de rastreamento sob demanda está sendo definida. Selecione aqueles que estão instalados em estações de trabalho clientes.

   OBSERVAÇÃO: a opção **Excluir esta seção de rastreamento sob demanda** desabilitará todas as configurações na janela para o tipo de produto selecionado - elas não serão aplicadas em estações de trabalho com o tipo de produto definido na **Seção de configuração**. Portanto, todos os clientes com o produto especificado serão excluídos da lista de destinatários. Se o administrador marcar clientes como receptores e excluir o produto usando o parâmetro mencionado acima, então a tarefa falhará com uma notificação de que a tarefa não pôde ser aplicada. Para evitar isso, o administrador sempre deve especificar clientes para os quais a tarefa será atribuída.

2) No **Nome do perfil**, você pode selecionar um perfil de rastreamento a ser aplicado à tarefa.

3) Na seção **Unidades a serem rastreadas**, selecione os tipos de unidades a serem rastreadas em computadores clientes. Se a seleção for muito geral, você poderá adicionar um caminho exato para objetos a serem rastreados. Use

o campo **Caminho** ou o botão **Adicionar caminho** para essa finalidade. Selecione **Limpar histórico** para restaurar a lista original de unidades a serem rastreadas.

4) Clique em **Avançar** para prosseguir para as janelas da caixa de diálogo rotuladas **Selecionar clientes** e **Relatório de tarefa**, que são descritas em detalhes no capítulo Tarefas 64.

5) Depois que a execução da tarefa for concluída nas estações de trabalho clientes, os resultados serão enviados de volta para o ERAS e eles poderão ser visualizados no ERAC no painel **Log de rastreamento**.

5.1.3 Tarefa Atualizar agora

A finalidade desta tarefa é forçar atualizações em estações de trabalho de destino (atualizações do banco de dados de vírus, bem como atualização de componentes do programa).

1) Clique com o botão direito do mouse em qualquer estação de trabalho do painel **Clientes** e selecione **Nova tarefa** > **Atualizar agora**.

2) Se você quiser excluir determinados tipos de produtos de segurança da ESET da tarefa, selecione-os no menu suspenso **Seção de configuração** e selecione a opção **Excluir desta seção da tarefa Atualizar**.

3) Para usar um perfil de atualização específico para a tarefa **Atualizar agora**, habilite a opção **Especificar nome de perfil** e selecione o perfil desejado. Você também pode selecionar **Nome do perfil definido pelo usuário** e inserir o nome do perfil; o valor do campo será retornado para o padrão se você clicar em **Limpar histórico**.

4) Em seguida, clique em **Avançar** para prosseguir para as janelas da caixa de diálogo, **Selecionar clientes** e **Relatório de tarefa**. Para obter uma descrição dessas caixas de diálogo , consulte o capítulo Tarefas 64.

5.1.4 Tarefa de script do SysInspector

A tarefa de script do SysInspector permite que você execute scripts em computadores de destino. Ele é utilizado para remover os objetos não desejados do sistema. Para obter mais detalhes, consulte a página de ajuda do ESET SysInspector 140.

1) Depois de concluir o estágio I e o estágio II descritos no capítulo Tarefas 64, clique em **Selecionar** para escolher um script a ser executado na estação de trabalho de destino.

2) Clique em **Exibir e editar** para ajustar o script.

3) Clique em **Avançar** para prosseguir para as janelas de caixa de diálogo **Selecionar clientes** e **Relatório de tarefa**, que são descritas no capítulo Tarefas 64.

4) Depois que a tarefa for concluída na estação de trabalho cliente, as informações serão exibidas na coluna **Estado** do painel **Tarefas**.

OBSERVAÇÃO: as tarefas de script do SysInspector são compatíveis somente com o ESET Smart Security/ESET NOD32 Antivirus versão 4.0 e posteriores.

5.1.5 Recursos de proteção

Esta tarefa permite que o administrador modifique o status dos recursos de proteção do produto de segurança (Produtos de segurança da ESET para Windows versão 5 e posteriores).

1. Há três fases para cada recurso de proteção - **Não alterar**, **Desativação temporária** e **Ativar**. Você pode alterná-las marcando a caixa de seleção ao lado de cada recurso. Se o recurso de proteção estiver sendo desativado (Desativação temporária), você poderá definir um **Intervalo de tempo de desativação temporária**. Esse intervalo pode ser de 10 minutos a **Até a próxima reinicialização** (desabilita o recurso totalmente até a próxima reinicialização do computador).

2. Em seguida, selecione os clientes para os quais você deseja modificar os recursos de proteção e conclua a tarefa 68.

OBSERVAÇÃO: tenha cautela ao desabilitar recursos de proteção, pois esse é um risco em potencial à segurança. O cliente será notificado sempre que um recurso de proteção for desabilitado.

5.1.6 Executar tarefa agendada

Esta tarefa acionará uma tarefa agendada que será executada imediatamente no cliente. Você pode selecionar uma tarefa **Predefinida** da agenda do cliente ou selecionar uma tarefa **Por ID**. Cada tarefa agendada tem uma ID, a fim de que você possa selecionar uma tarefa do menu suspenso ou digitar uma ID. Para visualizar cada tarefa na agenda em um cliente específico, inicie essa tarefa do menu de contexto na guia **Cliente**.

Selecione a tarefa que deseja executar em um cliente; em seguida, selecione os clientes para os quais deseja modificar os recursos de proteção e conclua a tarefa 68.

5.1.7 Restaurar/excluir da tarefa de quarentena

Com esta tarefa, você pode restaurar ou excluir objetos em quarentena especificados da quarentena do cliente.

1) Depois que você abrir a janela **Restaurar/excluir da quarentena** (consulte o capítulo Tarefas 64), selecione uma ação a ser realizada - seja **Restaurar** ou **Excluir** - no objeto em quarentena.

   OBSERVAÇÃO: Quando restaurar um objeto da quarentena que ainda seja detectado como uma ameaça, você pode querer considerar excluir este objeto de um próximo rastreamento usando a opção **Adicionar exclusão também** para evitar que o objeto seja rastreado e colocado em quarentena novamente. Note que nem todos os objetos podem ser excluídos, por exemplo: cavalos de tróia ou vírus. Tentar excluir esses arquivos causará um erro. Se quiser excluir arquivos limpos (não detectados como uma ameaça), faça isso diretamente no cliente ou usando o Editor de configuração ESET (política, tarefa, etc.)

2) Selecione uma condição pela qual objetos em quarentena serão restaurados/excluídos e clique em **Avançar**.

   OBSERVAÇÃO: Se você tiver aberto a janela Restaurar/excluir da Quarentena clicando com o botão direito do mouse em uma entrada de quarentena, diretamente da guia **Quarentena** (e selecionando **Restaurar/excluir da tarefa de quarentena**), você precisará especificar condições (a opção **Por hash** será automaticamente selecionada e o código hash do arquivo de quarentena será usado como um identificador).

3) Selecione os clientes para sua operação de restauração/exclusão (consulte o capítulo Tarefas 64) e clique em **Avançar** .

4) Revise suas configurações na janela **Relatório de tarefa**, insira um nome para sua tarefa, especifique o horário em que gostaria de aplicar a tarefa (e opções de limpeza, se desejado) e, em seguida, clique em **Concluir** para confirmar. Consulte o capítulo Tarefas 64 para obter mais informações.

5.1.8 Reversão de banco de dados de vírus

Se você suspeitar que uma nova atualização do banco de dados de vírus pode estar instável ou corrompida, poderá reverter para a versão anterior e desabilitar quaisquer atualizações por um período de tempo escolhido. Como alternativa, você pode habilitar atualizações desabilitadas anteriormente.

1) Desabilitar/habilitar atualizações do banco de dados de vírus

Desabilitar por X horas - o banco de dados de vírus dos clientes será revertido para as versões anteriores (com base em um instantâneo criado no cliente) e qualquer atualização para os clientes selecionados será desabilitada pelo período de tempo selecionado. Você também pode selecionar **Infinito** e desabilitar completamente as atualizações. Tenha cautela ao desabilitar totalmente atualizações do banco de dados, pois esse é um risco em potencial à segurança.

Aviso: a opção **Infinito** permanece ativa mesmo depois da reinicialização de um computador cliente.

Habilitar atualizações desabilitadas anteriormente - a atualização do banco de dados de vírus será habilitada novamente.

2) Selecione os clientes para esta tarefa e clique em **Avançar**.

3) Revise suas configurações na janela **Relatório de tarefa**, insira um nome para sua tarefa, especifique o horário em que gostaria de aplicar a tarefa (e opções de limpeza, se desejado) e, em seguida, clique em **Concluir** para confirmar. Consulte o capítulo Tarefas 64 para obter mais detalhes.

5.1.9 Limpar cache de atualização do cliente

Esta tarefa funciona para Produtos de segurança da ESET versão 5 e posteriores. Se você achar que a atualização do banco de dados de vírus não foi bem-sucedida, poderá apagar o cache de atualização do cliente e o download da atualização mais recente será feito novamente.

1) Inicie a tarefa e clique em **Avançar**.

2) Selecione os clientes para esta tarefa e clique em **Avançar**.

3) Revise suas configurações na janela **Relatório de tarefa**, insira um nome para sua tarefa, especifique o horário em que gostaria de aplicar a tarefa (e opções de limpeza, se desejado) e, em seguida, clique em **Concluir** para confirmar. Consulte o capítulo Tarefas 64 para obter mais detalhes.

5.1.10 Gerar tarefa de log de auditoria de segurança

Esta tarefa aplica-se somente ao ESET Mobile Security.

Verificações de auditoria de segurança: nível de bateria, status do Bluetooth, espaço livre em disco, visibilidade de dispositivo, rede doméstica e processos em execução. Um relatório detalhado será gerado, indicando se o valor do item está ou não abaixo do limite especificado ou se poderia representar um risco em potencial à segurança (p. ex., visibilidade de dispositivo ativada, etc.).

Para executar a auditoria de segurança no telefone:

1) Clique com o botão direito do mouse no nome do cliente no painel **Clientes** e selecione **Nova tarefa** > **Gerar log de auditoria de segurança** no menu de contexto.

2) Clique em **Avançar** para prosseguir para as janelas **Selecionar clientes** e **Relatório de tarefa**. Para obter uma descrição dessas janelas, consulte o capítulo intitulado Tarefas 64.

5.1.11 Mostrar tarefa de notificação

Esta tarefa aplica-se somente ao ESET Mobile Security.

Para enviar uma notificação (p. ex., uma mensagem de aviso) para o telefone:

1) Clique com o botão direito do mouse no nome do cliente no painel **Clientes** e selecione **Nova tarefa** > **Mostrar notificação** no menu de contexto.

2) Digite o **Título** da notificação e o **Corpo** da mensagem nos campos apropriados e selecione o **Detalhamento** da notificação.

3) Clique em **Avançar** para prosseguir para as janelas **Selecionar clientes** e **Relatório de tarefa**. Para obter uma descrição dessas janelas, consulte o capítulo intitulado Tarefas 64.

5.1.12 Concluindo a tarefa

Na última janela da caixa de diálogo, a visualização da tarefa será exibida. Ela contém todos os parâmetros de tarefa e permite que o usuário clique em **Voltar** e realize as modificações, se necessário.

A segunda parte da janela contém as seguintes configurações:

- **Nome** - O nome da tarefa.
- **Descrição** - Descrição da tarefa.
- **Aplicar tarefa após** - Tempo para implantar a tarefa em computadores clientes.
- **Excluir tarefas automaticamente por limpeza se concluídas com êxito** - exclui automaticamente todas as tarefas realizadas com êxito.

5.2 Gerenciador de grupos

O Gerenciador de grupos é uma ferramenta avançada para o gerenciamento de seus clientes, separando-os em diferentes grupos e aplicando diferentes configurações, tarefas, restrições, etc. Ele é facilmente acessado via **Ferramentas > Gerenciador de grupos** ou **CTRL+G**. Os grupos são independentes para cada ERAS e não são replicados.

Você pode criar seus próprios grupos para atender às suas necessidades na rede de sua empresa, ou simplesmente sincronizar os grupos do cliente ERAC com seu Microsoft Active Directory usando o caractere curinga **Sincronização do Active Directory** na janela principal do Gerenciador de grupos.

Há dois tipos principais de grupos clientes:

- Grupos estáticos 69
- Grupos paramétricos 70

Os grupos estáticos e paramétricos podem ser usados em vários locais no ERA, o que melhora significativamente as capacidades de gerenciamento do cliente.

5.2.1 Grupos estáticos

Grupos estáticos são criados para separar clientes em sua rede em grupos e subgrupos nomeados. Por exemplo, você pode criar um grupo de Marketing que terá todos os clientes e marketing e também criará subgrupos especializados - Vendas locais, Gerenciamento da região EMEA, etc.

A janela principal Grupos estáticos é dividida em duas partes. O lado esquerdo contém grupos e subgrupos existentes exibidos hierarquicamente. Os clientes incluídos no grupo selecionado serão relacionados no lado direito da janela. Por padrão, somente clientes no grupo selecionado serão relacionados. Se você quiser ver clientes incluídos em subgrupos do grupo atualmente selecionado, marque a caixa de seleção ao lado de **Mostrar clientes em subgrupos** no lado direito da janela.

Para criar um novo grupo, clique em **Criar** e insira um nome para o grupo. Um novo grupo será criado como um subgrupo do grupo pai atualmente selecionado. Se você quiser criar um novo grupo pai, selecione a raiz da árvore hierárquica - **Grupos estáticos**. O campo **Grupo pai** contém o nome do grupo pai do grupo recém-criado (ou seja, "/" para a raiz). Recomendamos o uso de um nome que indique onde os computadores estão localizados (p. ex., *Departamento comercial, Suporte* etc.). O campo Descrição pode ser usado para descrever melhor o grupo (p. ex., "*Computadores no escritório C*", "*Estações de trabalho da sede*", etc.). Grupos configurados e recém-criados também podem ser editados posteriormente.

OBSERVAÇÃO: quando uma tarefa é enviada para o grupo Pai, todas as estações de trabalho que pertencem a seus subgrupos também aceitarão essa tarefa.

Além disso, é possível criar grupos vazios para uso futuro.

Clique em **OK** para criar o grupo. Seu nome e descrição serão exibidos à esquerda e o botão **Adicionar/Remover** se tornará ativo. Clique nesse botão para adicionar clientes que gostaria que fossem incluídos no grupo (dê um duplo clique ou arraste e solte-os da esquerda para a direita). Para localizar e adicionar clientes, insira o nome completo do cliente ou parte dele no campo **Pesquisa rápida** e todos os clientes contendo a cadeia de caracteres digitada serão exibidos. Para marcar todos os clientes, clique em **Selecionar tudo**. Clique em **Atualizar** para verificar se há novos clientes recentemente conectados ao servidor.

Se a seleção manual dos clientes não for conveniente, você poderá clicar em **Adicionar especial...** para mais opções.

Selecione a opção **Adicionar clientes carregados no painel Clientes** para adicionar todos os clientes na seção de clientes ou selecione a opção **Somente selecionados**. Para adicionar clientes que já pertencem a outro servidor ou grupo, selecione-os das listas, à esquerda e à direita, e clique em **Adicionar**.

Clique em **OK** na janela da caixa de diálogo **Adicionar/Remover** para retornar à janela principal Gerenciador de grupos estáticos. O novo grupo deverá ser exibido com seus clientes correspondentes.

Clique em **Adicionar/Remover** para adicionar ou remover clientes de grupos, ou clique em **Excluir** para excluir um grupo inteiro. Clique em **Copiar para a área de transferência** para copiar as listas de clientes e grupos. Para atualizar os clientes do grupo, clique em **Atualizar**.

Você também pode **Importar/Exportar** clientes do grupo atualmente selecionado para um arquivo *.xml*.

5.2.2 Grupos paramétricos

Além de grupos estáticos, os grupos paramétricos também são muito úteis. As estações clientes serão atribuídas dinamicamente a um determinado grupo paramétrico quando as condições do grupo forem atendidas. A vantagem de grupos paramétricos é a capacidade de usá-los em vários locais, incluindo filtros, políticas, relatórios e notificações.

A janela principal Grupos paramétricos é composta por quatro seções. A opção **Grupos paramétricos** relaciona os principais grupos e subgrupos que foram criados. Quando você tiver selecionado um determinado grupo da lista **Grupos paramétricos**, os clientes que pertencerem ao grupo atualmente selecionado serão relacionados na seção **Grupo selecionado**.

OBSERVAÇÃO: quando um grupo pai for selecionado, a lista terá também os membros do subgrupo.

Os parâmetros definidos para um grupo selecionado serão relacionados na seção **Parâmetros** da janela. Você pode editar ou adicionar parâmetros a qualquer momento clicando em **Editar...**.

A seção **Status de sincronização** exibirá uma barra de andamento para o processo de sincronização.

1. Para criar um novo grupo, clique em **Criar...**. O novo grupo será criado como um subgrupo do grupo pai atualmente selecionado. Se você quiser criar um grupo principal, selecione a raiz da árvore hierárquica - **Grupos paramétricos**. O campo **Grupo pai** contém o nome do grupo pai do grupo recém-criado (ou seja, "/" para a raiz). Insira um **Nome** e uma breve **Descrição** para o novo grupo.
2. A próxima etapa é criar **Parâmetros de filtro do cliente**, que podem ser feitos no **Editor de regras** selecionando opções após clicar em **Editar...** Aqui, você pode especificar as condições necessárias para a regra ser acionada e aplicada. Selecione a condição e a especifique clicando em **Especificar** ao lado da regra na janela **Parâmetros** a seguir. Você também pode escolher se deseja que essa regra seja aplicada somente quando **todas as condições forem atendidas** ou se **qualquer uma das condições for atendida**.
3. Se você marcar a caixa de seleção ao lado de **Adesivo**, os clientes serão automaticamente adicionados a esse grupo quando eles corresponderem às condições, mas nunca serão removidos. O conteúdo de um grupo adesivo pode ser redefinido manualmente no nível de raiz.

OBSERVAÇÃO: esse parâmetro pode ser definido somente ao criar um novo grupo.

Para editar um grupo existente, selecione-o da lista **Grupos paramétricos** e então clique em **Editar...** na parte inferior da janela. Para exclusão de grupo, selecione o grupo desejado e clique em **Excluir**.

Você pode atualizar manualmente a lista de grupos clicando em **Atualizar**. Para importar um grupo de um arquivo, selecione um grupo na seção **Grupos paramétricos** na qual você deseja que o novo grupo seja importado e clique em **Importar...** Confirme sua seleção clicando em **Sim**. Localize o arquivo que deseja importar e clique em **Abrir**. O grupo (e todos os seus subgrupos) serão importados no local selecionado. Para exportar um grupo (e todos os seus subgrupos), selecione-o na seção **Grupos paramétricos**, clique na seta em **Importar...** e selecione **Exportar...**. Clique em **Sim** para confirmar, selecione um nome e local para seu arquivo de exportação e clique em **Salvar**.

OBSERVAÇÃO: você pode usar seu mouse para arrastar e soltar grupos que já estão na seção **Grupos paramétricos**.

OBSERVAÇÃO: você pode usar os grupos paramétricos de forma conveniente para filtrar dados ou clientes. Por exemplo, talvez você queira gerar relatórios somente para computadores com Windows XP. Crie um grupo paramétrico somente para computadores com o sistema operacional específico e use esse grupo no alvo de filtro. Você também pode definir seus próprios **Dados personalizados de cliente** ao criar um pacote de instalação 44 - (**Editor de configuração** > **Kernel** > **Configurações** > **Administração remota**). Defina essa opção (Dados personalizados de cliente) como um parâmetro para um grupo paramétrico e cada usuário que instalar esse pacote se tornará um membro desse grupo.

5.2.3 Sincronização do Active Directory / LDAP

A Sincronização do Active Directory utiliza a criação automática de grupos (com clientes correspondentes) com base na estrutura definida pelo Active Directory. Ela permite que o administrador classifique clientes em grupos, desde que o nome do cliente corresponda ao tipo de objeto *computador* no Active Directory (AD) e pertença a grupos no AD.

Há duas opções principais que determinam a forma de sincronização:

- **Sincronizar grupos** permite que você escolha quais grupos do AD serão sincronizados. Selecione **Todos os grupos** para sincronizar a estrutura completa da árvore do AD, independentemente de os grupos do AD terem ou não clientes ERA. As próximas duas opções (**Somente grupos contendo clientes do ERA Server** e **Somente grupos contendo clientes do servidor principal do ERA**) vão sincronizar somente grupos contendo clientes ERA existentes.
- A opção **Tipo de sincronização** definirá se os grupos do AD serão sincronizados aos grupos do AD/LDAP existentes (

Importação de grupos do AD/LDAP) ou se os grupos do AD/LDAP existentes serão totalmente substituídos por aqueles a serem sincronizados (**Grupos do AD/LDAP a sincronizar**).

- **Ramificações sincronizadas** permite que você selecione ramificações específicas do **Active Directory/LDAP** a serem sincronizadas. Clique em **Configurar** para selecionar quais ramificações do Active Directory/LDAP serão sincronizadas com os grupos. Por padrão, todos os ramais são marcados/selecionados.

Observação: Clique em **Mais informações!** para exibir informações adicionais sobre as configurações e regras de Sincronização do Active Directory / LDAP.

- Para configurar o intervalo de sincronização entre o AD/LDAP e o Servidor ERA, clique em **Alterar** perto da opção Sincronizar. Selecione a frequência de sincronização desejada na janela de diálogo do **AD/LDAP Intervalo agendado de sincronização do AD (no horário local do servidor)**. A frequência selecionada será exibida perto da opção **Sincronizar**.

A configuração detalhada da sincronização do Active Directory pode ser realizada usando o **Editor de Configuração** (**Administrador Remoto** > **ERA Server** > **Configurações** > **Grupos** e **Active directory / LDAP**). Você pode adicionar outros objetos do Active Directory/LDAP marcando a(s) caixa(s) de seleção ao lado da(s) opção(ões) desejada(s).

Clicar em **Sincronizar agora** inicia a sincronização (com base nas opções configuradas acima).

OBSERVAÇÃO: para que o ERAS seja sincronizado com o Active Directory, o ERAS não precisa ser instalado em seu controlador de domínio. O controlador de domínio precisa estar acessível somente do computador no qual seu ERAS está localizado. Para configurar a autenticação no seu controlador de domínio, vá para **Ferramentas** > **Opções de servidor** > **Avançado** > **Editar configurações avançadas** > **Administrador remoto** > **ERA Server** > **Configurações** > **Active directory / LDAP**.

5.3 Políticas

As políticas são de muitas formas semelhantes a **Tarefas de configuração**, exceto que não são tarefas monoestáveis enviadas para uma ou mais estações de trabalho. Em vez disso, elas fornecem manutenção contínua de determinadas definições de configuração para produtos de segurança da ESET. Em outras palavras, uma **Política** é uma configuração é que imposta a um cliente.

5.3.1 Princípios básicos e operação

Acesse o Gerenciador de políticas selecionando **Ferramentas** > **Gerenciador de políticas...** A Árvore de política à esquerda relaciona as políticas que estão presentes em servidores individuais. O lado direito é dividido em quatro seções - **Configurações de política**, **Configuração de política**, **Ação de política** e **Configurações de política global** - as opções nessas seções permitem que um administrador gerencie e configure políticas.

As funções principais do Gerenciador de políticas incluem a criação, a edição e a remoção de políticas. Os clientes recebem políticas do ERAS. O ERAS pode usar várias políticas, que podem herdar configurações umas das outras ou de políticas de um servidor superior.

O sistema de adoção de políticas de um servidor superior é denominado *herança*; políticas que são criadas como resultado de herança são referidas como *políticas mescladas*. A herança é baseada no princípio pai-filho, ou seja, uma política filha herda configurações de uma política pai.

5.3.2 Como criar políticas

A instalação padrão implementa somente uma política chamada "Política do servidor". A política em si é configurável no Editor de configuração da ESET - clique em **Editar política...** e defina parâmetros para o produto (ou cliente) de segurança da ESET selecionado. Todos os parâmetros são organizados em uma estrutura abrangente e todos os itens no Editor recebem um ícone. Os clientes adotarão somente parâmetros ativos (marcados por um ícone azul). Todos os parâmetros inativos (esmaecidos) permanecerão inalterados em computadores de destino. O mesmo princípio se aplica a políticas herdadas e mescladas - uma política filha adotará somente parâmetros ativos de uma política pai.

ERA Servers permite várias políticas (**Nova política filho...**). As seguintes opções estão disponíveis para novas políticas: **Nome da política**, com ligação para uma **Política pai** e **Configuração de política** (a configuração pode estar vazia, você pode copiar a configuração de política mesclada a partir de uma política no menu suspenso, copiar de um arquivo de configuração *.xml* ou usar o **Assistente de mescla de regras de firewall**). Políticas podem ser criadas somente no servidor no qual você está atualmente conectado via ERAC. Para criar uma política em um servidor inferior, será necessário conectar-se diretamente a esse servidor.

Cada política tem dois atributos básicos: **Substituir qualquer política filha** e **Política replicável para baixo**. Esses

atributos definem como os parâmetros de configuração ativos são adotados por políticas filhas.

- **Substituir qualquer política filha** - aplica todos os parâmetros ativos em políticas herdadas. Se a política filha diferir, a política mesclada conterá todos os parâmetros ativos da política pai (mesmo que a opção **Substituir...** esteja ativa para a política filha). Todos os parâmetros inativos da política pai serão ajustados para combinar com a política filha. Se o atributo **Substituir qualquer política filha** não estiver habilitado, as configurações na política filha terão prioridade em relação àquelas na política pai para a política mesclada resultante. Essas políticas mescladas serão aplicadas a quaisquer políticas filho adicionais da política que foi editada.
- **Política replicável para baixo** - ativa a replicação de políticas para servidores inferiores, por exemplo, uma política pode servir como política padrão para servidores inferiores e também pode ser atribuída a clientes conectados a servidores inferiores.

As políticas também podem ser exportadas/importadas de/para um arquivo *.xml* ou importadas de grupos. Para obter mais informações, consulte o capítulo intitulado Importando/exportando políticas 73.

5.3.3 Políticas virtuais

Além das políticas criadas, bem como as replicadas de outros servidores (consulte o capítulo guia Replicação 99), a Árvore de política também contém uma política pai padrão, que é referida como uma política virtual.

A política pai padrão está localizada em um servidor superior nas configurações de política **Global** e selecionada como **Política padrão para servidores inferiores**. Se o servidor não for replicado, essa política estará vazia (será explicada posteriormente).

A política de clientes primários padrão está localizada no servidor determinado (não em um servidor superior) nas configurações de Política global e selecionada na política padrão para clientes primários. Ela é automaticamente aplicada a clientes recém-conectados (clientes primários) do ERAS especificado, exceto se já tiverem adotado alguma outra política de Regras de política (para obter mais informações, consulte o capítulo Atribuindo políticas a clientes 74). Políticas virtuais são links para outras políticas localizadas no mesmo servidor.

5.3.4 Função e finalidade de políticas na estrutura em árvore de política

Cada política na **Árvore de política** recebe um ícone à esquerda. O significado de ícones é o seguinte:

1) Políticas com ícones azuis referem-se àquelas presentes no servidor especificado. Há três subgrupos de ícones azuis:

Ícones com destinos brancos - a política foi criada nesse servidor. Além disso, não é replicável para baixo, o que significa que não é atribuída a clientes de servidores inferiores e também não serve como uma política pai para os servidores filhos. Essas políticas podem ser aplicadas somente no servidor - para clientes conectados ao servidor. Ela também pode servir como uma política pai para outra política do mesmo servidor.

Ícones com destinos azuis - a política também foi criada no servidor; no entanto, a opção **Substituir qualquer política filha** é selecionada (para obter mais informações, consulte o capítulo Como criar políticas 71).

Ícones com setas para baixo - essas políticas são replicadas e a opção **Política replicável para baixo** está habilitada. Você pode aplicar essas políticas no servidor especificado e em seus servidores filhos.

Ícones do para a **Política de servidor** padrão.

2) Políticas com ícones cinzas se originam de outros servidores.

Ícones com setas para cima - essas políticas são replicadas de servidores filhos. Elas podem ser visualizadas ou excluídas somente com a opção **Excluir ramificação de política**. Essa opção não excluirá a política em si. Ela removerá somente a política da Árvore de política. Portanto, elas podem reaparecer após a replicação. Se você não quiser exibir políticas de servidores inferiores, use a opção **Ocultar políticas de servidor externo não usado na árvore de políticas**.

Ícones com setas para baixo - essas políticas são replicadas de servidores superiores. Elas podem ser usadas como políticas pai para outras políticas, atribuídas a clientes (**Adicionar clientes**) ou removidas (**Excluir política**). Observe que excluir excluirá somente a política - ela será exibida novamente depois da replicação do servidor superior (exceto se o atributo **Política replicável para baixo** tiver sido desabilitado no servidor superior).

OBSERVAÇÃO: para mover e atribuir políticas na estrutura, você pode selecionar a política pai ou arrastá-la e soltá-la com o mouse.

As regras de políticas existentes podem ser importadas/exportadas de/para um arquivo *.xml* ao clicar no botão **Importar/Exportar políticas**. Se uma política existente e importada tiverem o mesmo nome, uma cadeia de caracteres

aleatória será adicionada automaticamente após o nome de uma política importada.

5.3.5 Visualizando políticas

As políticas na estrutura **Árvore de política** podem ser visualizadas diretamente no **Editor de configuração** clicando em **Exibir política** > **Exibir...** ou **Exibir mesclado...**.

Exibir mesclado - exibe a política mesclada criada como resultado da herança (o processo de herança aplica configurações da política pai). Essa opção é exibida por padrão, pois a política atual já é uma política mesclada.

Exibir - exibe a política original antes de ela ter sido mesclada em uma política pai.

Em servidores inferiores, as seguintes opções estão disponíveis para políticas herdadas de servidores superiores:

Exibir mesclado - mesmo que acima.

Exibir parte de substituição - esse botão se aplica a políticas com o atributo **Substituir qualquer política filha**. Essa opção mostra somente a parte forçada da política - ou seja, a que tem prioridade em relação a outras configurações em políticas filhas.

Exibir parte não forçada - tem efeito oposto a Exibir parte de substituição - exibe somente itens ativos aos quais a opção Substituir... não se aplica.

OBSERVAÇÃO: você pode dar um duplo clique em um item da árvore de política para exibição mesclada.

5.3.6 Importando/exportando políticas

O Gerenciador de políticas permite que você importe/exporte políticas e regras de política. As políticas existentes podem ser importadas/exportadas de/para um arquivo *.xml* ao clicar no botão **Importar/Exportar políticas**. As políticas ainda podem ser importadas de grupos ao clicar no botão **Importar de grupos...**. As regras de política podem ser importadas/exportadas ao clicar no botão **Importar...** ou **Exportar...** e, além disso, elas podem ser criadas usando o **Assistente de regras de política**.

Os conflitos de nome (os nomes de políticas existentes e importadas são idênticos) são resolvidos durante a importação ao acrescentar uma cadeia de caracteres aleatória ao nome da política importada. Se um conflito não puder ser resolvido dessa forma (geralmente devido ao fato de o novo nome ser muito longo), a importação será concluída com o aviso *Conflito de nome de política não resolvido*. A solução será excluir ou renomear as regras de política ou políticas em conflito.

5.3.7 Assistente de migração de política

Este **Assistente de migração de política** vai ajudá-lo a criar uma nova **Política de Windows desktop v5**, ou a atualizar sua política **Windows desktop v5** existente usando as configurações de suas políticas existentes da linha de produto do Windows v3 e v4. É possível migrar todas as políticas durante a instalação sobre uma versão anterior, mas para personalizar todas as configurações para migração recomendamos que use o **Assistente de migração de política**.

Para migrar políticas:

1. Selecione a(s) caixa(s) de marcação próxima(s) das políticas das quais você deseja migrar configurações.
2. Se uma Política de Ponto de Extremidade já existir, selecione uma das configurações a seguir:

- **Substituir política existente de Ponto de extremidade e usar apenas as configurações de origem** - A política existente será completamente substituída pela política recém-criada (**Windows desktop v5**) e as configurações da política original (**Linha de produto do Windows v3 e v4**) serão usadas.
- **Mesclar políticas e não substituir configurações conflitantes de Ponto de extremidade** - Políticas existentes e migradas serão mescladas e configurações existentes da política de Windows Desktop v5 não serão substituídas pelas configurações da política de Linha de produto do Windows v3 e v4.
- **Mesclar políticas e substituir configurações conflitantes de Ponto de extremidade** - Políticas existentes e migradas serão mescladas e as configurações em conflito serão substituídas pelas configurações originais (v3/v4).

3. Aguarde o final fo processo, o tempo vai variar dependendo do número de políticas sendo migradas. Clique em **Concluir** quando receber a mensagem **Migração de política concluída**.

5.3.8 Atribuindo políticas a clientes

Há duas regras principais para atribuir políticas a clientes:

1. Aos clientes locais (primários) pode ser atribuída qualquer política local ou qualquer política replicada de servidores superiores.
2. Aos clientes replicados de servidores inferiores pode ser atribuída qualquer política local com o atributo **Replicável para baixo** ou qualquer política replicada de servidores superiores. Eles não poderão ser forçados a adotar políticas de seu próprio servidor primário (para fazer isso, você deverá se conectar a esse servidor com o ERAC).

Um recurso importante é que cada cliente recebe alguma política (não há clientes sem política). Além disso, você não pode retirar uma política de um cliente. Você somente pode substituí-la por outra política. Se você não quiser aplicar uma configuração de qualquer política a um cliente, crie uma política em branco.

5.3.8.1 Política de clientes primários padrão

Um método de atribuição de políticas é a aplicação automática da **Política de servidor**, uma política virtual que é configurável nas configurações de política **Global**. Essa política é aplicada a clientes primários, ou sejam, aqueles diretamente conectados a esse ERAS. Para obter mais informações, consulte o capítulo Políticas virtuais 72.

5.3.8.2 Atribuição manual

Há duas maneiras de atribuir políticas manualmente: clicar com o botão direito do mouse em um cliente no painel **Clientes** e selecionar **Definir política** no menu de contexto ou clicar em **Adicionar clientes** > **Adicionar/Remover** no Gerenciador de políticas.

Clicar em **Adicionar clientes** no Gerenciador de políticas abrirá a janela da caixa de diálogo **Definir/Remover**. Os clientes são relacionados à esquerda no formato Servidor/Cliente. Se a opção **Política replicável para baixo** for selecionada, a janela também relacionará clientes replicados de servidores inferiores. Selecione clientes para receber a política usando o método de arrastar e soltar ou clicando em **>>** para movê-los para **Itens selecionados**. Clientes recentemente selecionados terão um asterisco amarelo e ainda poderão ser removidos de **Itens selecionados** clicando no botão **<<** ou **C**. Clique em **OK** para confirmar a seleção.

OBSERVAÇÃO: depois de confirmar, se você reabrir a janela da caixa de diálogo **Definir/Remover**, os clientes não poderão ser removidos de **Itens selecionados**, você poderá apenas substituir a política.

Você também pode adicionar clientes usando o recurso **Adicionar especial**, que pode adicionar todos os clientes de uma só vez, adicionar clientes selecionados ou adicionar clientes de grupos ou servidores selecionados.

5.3.8.3 Regras de política

A ferramenta **Regras de política** permite que um administrador atribua automaticamente políticas para estações de trabalho clientes de forma mais abrangente. As regras são aplicadas imediatamente depois que o cliente se conecta ao servidor; elas têm prioridade sobre a **Política do servidor** e sobre a atribuição manual. A opção **Política de servidor** aplica-se somente se o cliente não se encaixar em qualquer uma das regras atuais. Da mesma forma, se houver uma política atribuída manualmente a ser aplicada e ela estiver em conflito com as regras de política, a configuração forçada pelas regras de política terá precedência.

Se cada servidor for gerenciado por um administrador local, cada administrador poderá criar regras de políticas individuais para seus clientes. Nesse cenário, é importante que não haja conflitos entre regras de políticas, como quando o servidor superior atribui uma política a clientes com base nas regras de políticas, enquanto o servidor inferior atribui simultaneamente políticas separadas com base nas regras de políticas locais.

As regras de políticas podem ser criadas e gerenciadas na guia **Regras de política** no Gerenciador de políticas. O processo de criação e aplicação é muito semelhante ao da criação e gerenciamento de regras em clientes de email: cada regra pode conter um ou mais critérios; quanto mais no início da lista a regra estiver, mais importante ela será (ela poderá ser movida para cima ou para baixo).

Para criar uma nova regra, clique em **Nova regra** e selecione se deseja **Criar nova** ou usar o Assistente de regras de política 75. Em seguida, insira um **Nome**, **Descrição**, **Parâmetro de filtro de cliente** e **Política** (uma política que será aplicada a quaisquer clientes correspondendo aos critérios especificados).

Para configurar os critérios de filtragem, clique no botão **Editar**:

(NÃO) DO servidor primário - se (não) localizado no servidor primário.
(NÃO) É novo cliente - se (não) for um novo cliente.
(NÃO) TEM sinalizador Novo - aplica-se a clientes com/sem o sinalizador Novo cliente.
Servidor primário (NÃO) incluído (especifique) - se o nome do servidor primário tiver/não tiver...
GRUPOS DO ERA INCLUÍDOS (especifique) - se o cliente pertencer ao grupo...
GRUPOS DO ERA NÃO INCLUÍDOS (especifique) - se o cliente não pertencer ao grupo...
DOMÍNIO/GRUPO DE TRABALHO (NÃO) EM (especifique) - se o cliente pertencer/não pertencer ao domínio...
Máscara de nome de computador (especifique) - se o nome de computador for...
TEM máscara IPv4 (especifique) - se o cliente pertencer ao grupo definido pela máscara e endereço IPv4...
TEM intervalo IPv4 (especifique) - se o cliente pertencer ao grupo definido pelo intervalo IPv4...
TEM máscara IPv6 (especifique) - se o cliente pertencer ao grupo definido pela máscara e endereço IPv6...
TEM intervalo IPv6 (especifique) - se o cliente pertencer ao grupo definido pelo intervalo IPv6...
(NÃO) TEM política definida (especifique) - se o cliente adotar (ou não) a política...
Nome do produto (NÃO) EM - se o nome do produto for...
A versão do produto (NÃO) É - se a versão do produto for...
Máscara de informações personalizadas de cliente 1, 2, 3 (NÃO) INCLUÍDA - se as informações personalizadas de cliente tiverem...
Máscara de comentário de cliente (NOT) IN -
(NÃO) TEM status de proteção (especifique) - se o status de proteção do cliente for...
A versão do banco de dados de assinatura de vírus (NÃO) É - se o banco de dados de assinatura de vírus for...
A última conexão É (NÃO) anterior a (especifique) - se a última conexão for anterior a...
ESTÁ (NÃO) aguardando reinicialização - se o cliente estiver aguardando reinicialização.

Regras de política podem ser importadas ou exportadas para um arquivo *.xml*. Regras de política também podem ser criadas automaticamente usando o Assistente de regras de política 75, que permite que você crie uma estrutura de política com base na estrutura de grupo existente e então mapeie políticas criadas para grupos ao criar regras de política correspondentes. Para obter mais informações sobre a importação/exportação de regras de políticas, consulte o capítulo intitulado Importando/exportando políticas 73.

Para remover uma regra de política, clique no botão **Excluir regra...**.

Clique em **Executar regra de política agora...** se quiser aplicar imediatamente a regra ativada.

5.3.8.3.1 Assistente de regras de política

O Assistente de regras de política permite que você crie uma estrutura de política com base na estrutura de grupo existente, bem como que você mapeie políticas criadas para grupos ao criar regras de política correspondentes.

1. Na primeira etapa, será solicitado que você organize seu grupo. Se você não tiver uma configuração de estrutura de grupo desejada, poderá clicar no Gerenciador de grupos 69 para configurar seus grupos e, em seguida, clicar em **Avançar**.
2. Na segunda etapa, será solicitado que você especifique quais das categorias de grupos clientes serão afetadas pela nova regra de política. Depois de selecionar as caixas de seleção desejadas, clique em **Avançar**.
3. Escolha a **Política pai**.
4. Na etapa final, você verá uma email de status de processo simples. Clique em **Concluir** para fechar a janela **Assistente de regras de política**.

Sua nova regra de política aparecerá na lista na guia **Regras de política**. Marque a caixa de seleção ao lado do nome de sua regra para ativar uma regra específica.

Para obter mais informações sobre a importação/exportação de regras de políticas e conflitos de nome, consulte o capítulo intitulado Importando/exportando políticas 73.

5.3.9 Políticas para clientes móveis

Um usuário com um produto ESET instalado no seu dispositivo móvel tem mais controle sobre as configurações e o comportamento de seu software do que um usuário com um notebook/desktop com um produto ESET instalado. Por isso não há necessidade de forçar continuamente uma política para usuários móveis, pois o usuário pode querer alterar ou ajustar algumas configurações. Recomendamos usar a técnica demonstrada abaixo para criar uma política para clientes móveis:

Crie uma política vazia (política padrão para clientes)

1. Clique em **Ferramentas > Gerenciador de Política**.
2. Clique em **Adicionar nova política** para criar uma política vazia, sem configurações modificadas. Na seção de Configuração de política, selecione **Criar configuração de política vazia**.
3. Clique em **Adicionar clientes** e selecione os usuários móveis que você deseja gerenciar com esta política.
4. Clique na guia Regras de política 74 e clique em **Nova**.
5. Selecione esta política no menu suspenso **Política** e clique em **Editar**.
6. Selecione a condição de regra **Novo cliente IS** no campo Parâmetros clique em IS para alterar a condição da regra para Novo cliente IS NOT, então clique em OK duas vezes.
7. Clique em OK e em Sim quando perguntado se deseja salvar suas configurações.
8. Esta política será aplicada ao cliente cada vez que se conectar ao ERA.

Criar uma política individual (política inicial para clientes)

1. Clique em **Ferramentas > Gerenciador de Política**.
2. Clique em **Adicionar nova política** para criar uma política vazia, sem configurações modificadas. Na seção de Configuração de política, selecione **Criar configuração de política vazia**.
3. Defina as configurações que você deseja aplicar para clientes móveis e salve a configuração.
4. Clique em **Adicionar clientes** e determine os usuários móveis que você deseja gerenciar com esta política.
5. Clique na guia Regras de política 74 e clique em **Nova**.
6. Selecione esta política no menu suspenso **Política** e clique em **Editar**.
7. Selecione a condição de regra **Novo cliente IS** e clique em OK duas vezes.
8. Clique em OK e em Sim quando perguntado se deseja salvar suas configurações.

Quando os clientes móveis conectarem ao ERA pela primeira vez, eles recebem as configurações da **Política individual** . A próxima vez que conectarem ao ERA, eles recebem uma **Política vazia** e suas configurações não serão afetadas.

5.3.10 Excluindo políticas

Como com a criação de regras, a exclusão é possível somente para políticas localizadas no servidor ao qual você está atualmente conectado. Para excluir políticas de outros servidores, você deve conectar-se diretamente a eles com o ERAC.

OBSERVAÇÃO: uma política pode ser vinculada a outros servidores ou políticas (como uma política pai, como uma política padrão para servidores inferior, como uma política padrão para clientes primários, etc.); portanto, em alguns casos seria necessário substituí-la em vez de excluí-la. Para ver opções para excluir e substituir, clique no botão **Excluir política...**. As opções descritas a seguir podem ou não estar disponíveis, dependendo da posição da política especificada na hierarquia de política.

- **Nova política para clientes primários com a política atualmente excluída** - permite que você selecione uma nova política para que clientes primários substituam a que você está excluindo. Os clientes primários podem adotar a **Política padrão para clientes primários**, bem como outras políticas do mesmo servidor (sejam atribuídas manualmente - **Adicionar clientes** ou impostas por **Regras de política**). Como uma substituição, você pode usar qualquer política do servidor especificado ou uma política replicada.
- **Nova política pai para as políticas filho da política atualmente excluída** - se uma política a ser excluída tiver servido como uma política pai para outras políticas filho, ela também deverá ser substituída. Ela poderá ser

substituída por uma política desse servidor, por uma política replicada de servidores superiores ou pelo sinalizador N/D, o que significa que políticas filho não receberão uma política substituta. Recomendamos que você atribua uma substituta mesmo se não houver política filha. Outro usuário atribuindo uma política filha a essa política durante o processo de exclusão causaria um conflito.

- **Nova política para clientes replicados com a política atualmente excluída ou modificada** - aqui, você pode selecionar uma nova política para clientes replicados de servidores inferiores - aqueles que foram aplicados àquela que você está atualmente excluindo. Como uma substituição, você pode usar qualquer política do servidor especificado ou uma política replicada.
- **Nova política padrão para servidores inferiores** - se a política excluída servir como uma política virtual (consulte a seção **Configurações de política global**), ela deverá ser substituída por outra (para obter mais informações, consulte o capítulo Políticas virtuais 72). Como uma substituição, você pode usar qualquer política do servidor especificado ou um sinalizador N/D.
- **Nova política padrão para clientes primários** - se a política excluída servir como uma política virtual (consulte a seção **Configurações de política global**), ela deverá ser substituída por outra (para obter mais informações, consulte o capítulo Políticas virtuais 72). Você pode usar uma política do mesmo servidor como uma substituição.

A mesma caixa de diálogo também será aberta se você desabilitar a opção **Replicável para baixo** para uma política e clicar em **OK, aplicar** ou se você selecionar outra política da árvore de política. Isso ativará os itens **Nova política para clientes replicados com a política atualmente excluída ou modificada** ou **Nova política padrão para servidores inferiores**.

5.3.11 Configurações especiais

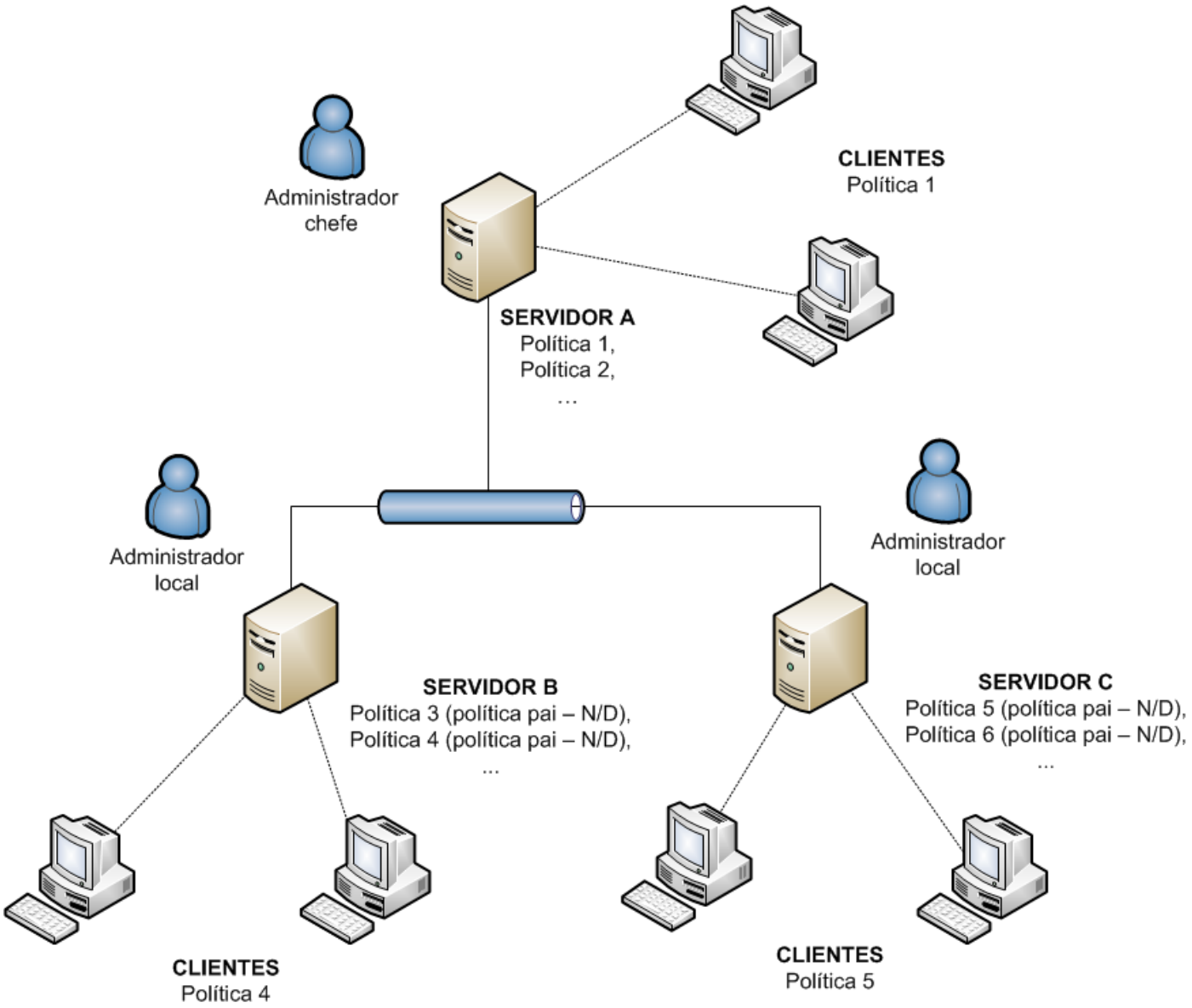
Duas políticas adicionais não estão localizadas no Gerenciador de políticas, mas em **Ferramentas** > **Opções do servidor** > **Avançadas** > **Editar configurações avançadas** > **ESET Remote Administrator** > **ERA Server** > **Configuração** > **Políticas**.

- **Intervalo para aplicação de política (minutos)** - Esse recurso se aplica a políticas no intervalo especificado. Recomendamos a configuração padrão.
- **Desativar uso de política** - habilite essa opção para cancelar a aplicação de políticas a servidores. Recomendamos essa opção se houver um problema com a política. Se você quiser evitar a aplicação de uma política a alguns clientes, uma solução melhor seria atribuir a eles uma política em branco.

5.3.12 Cenários de implantação de política

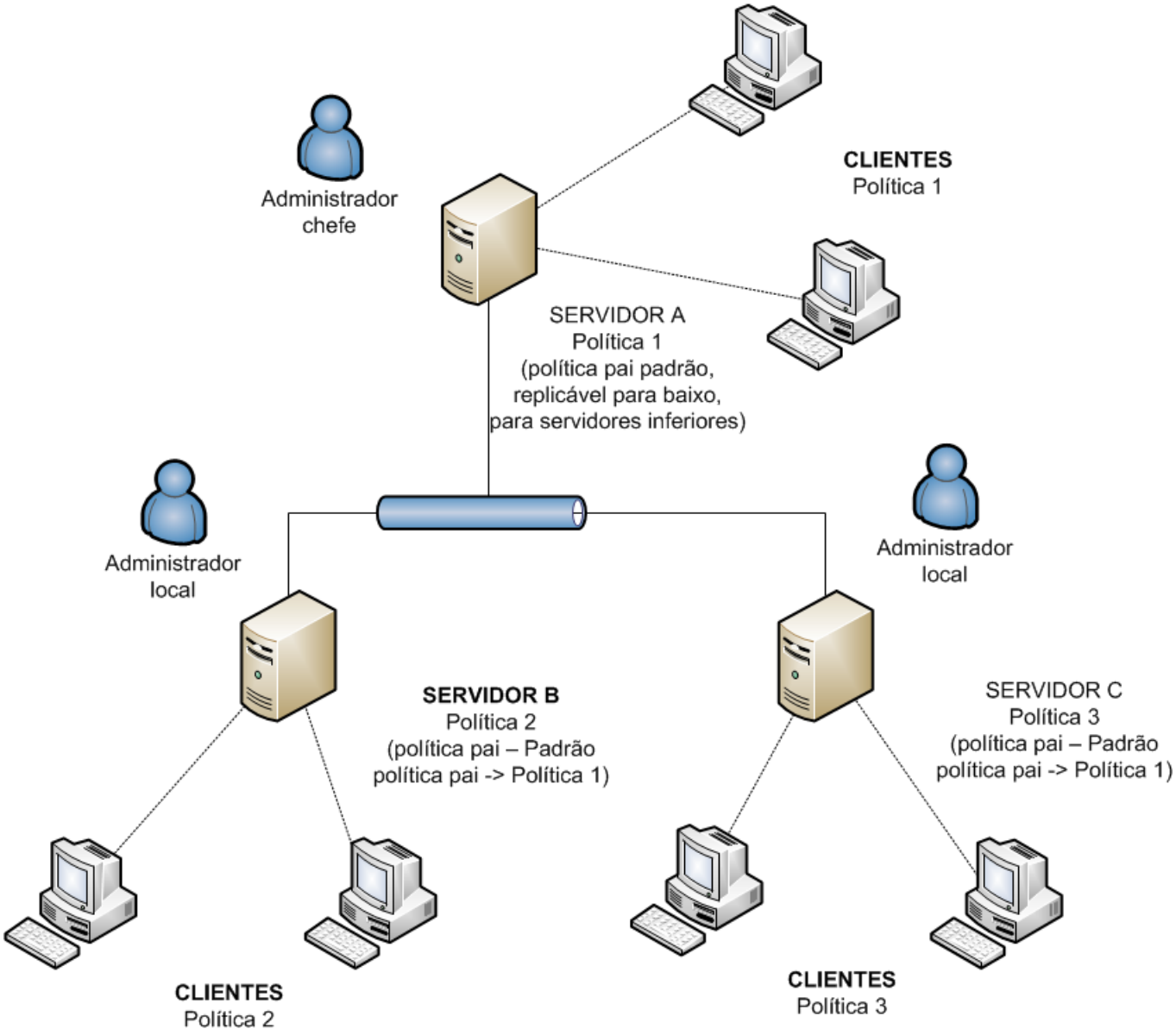
5.3.12.1 Cada servidor é uma unidade autônoma e as políticas são definidas localmente

Para a finalidade desse cenário, suponha que haja uma pequena rede com um servidor principal e dois servidores inferiores. Cada servidor tem vários clientes. Em cada servidor, há pelo menos uma ou mais políticas criadas. Os servidores inferiores estão localizados nas filiais da empresa; ambos os servidores são gerenciados por seus administradores locais. Cada administrador decide quais políticas serão atribuídas a quais clientes em seus servidores. O administrador principal não interfere nas configurações feitas pelos administradores locais e ele não atribui quaisquer políticas para clientes de seus servidores. De uma perspectiva de política do servidor, isso significa que o Servidor A não tem **Política padrão para servidores inferiores**. Isso também significa que o Servidor B e o Servidor C têm o sinalizador N/D ou outra política local (além da **Política pai padrão**) definida como uma política pai (p. ex., Servidores B e C não têm quaisquer políticas pai atribuídas do servidor superior).



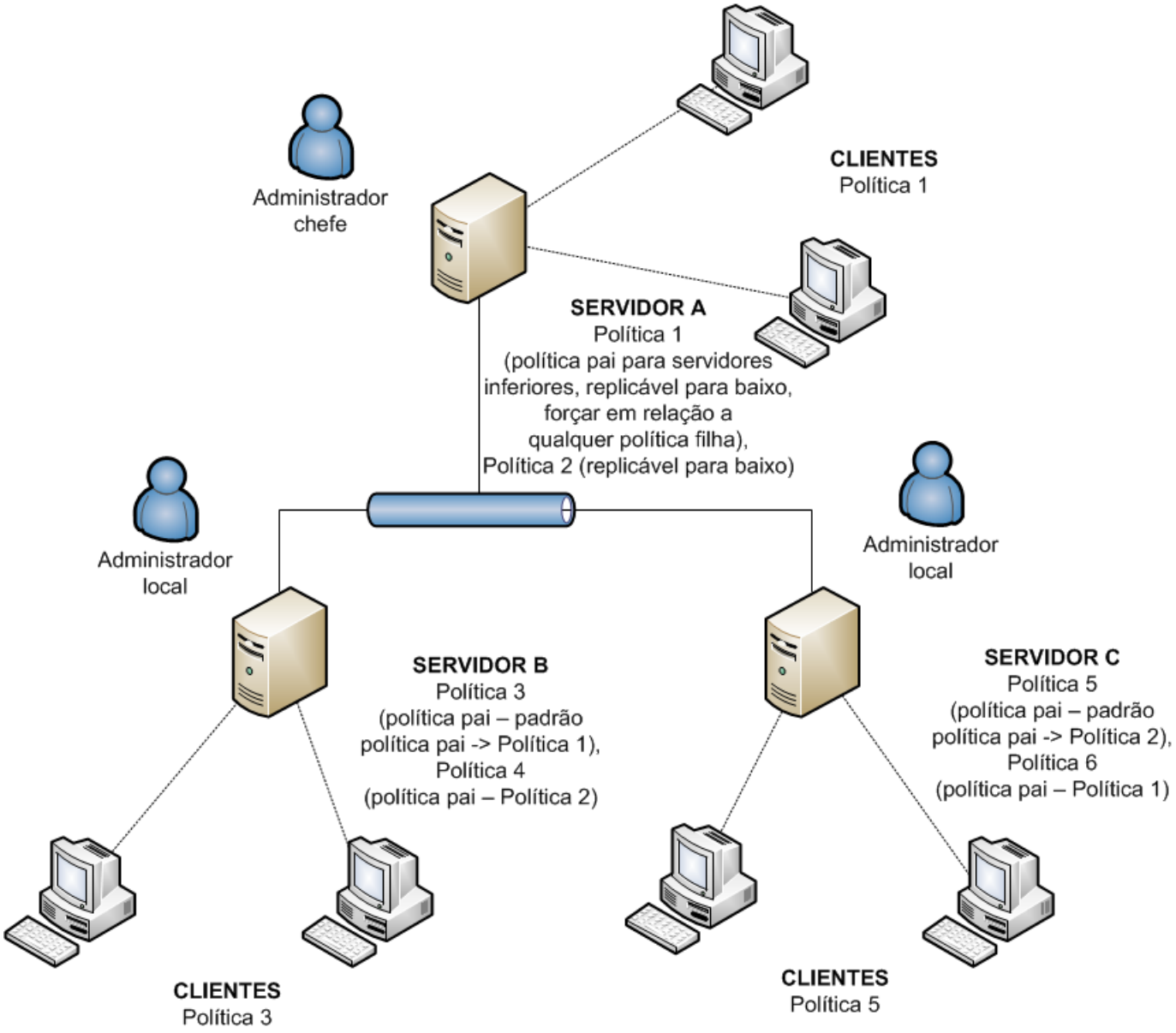
5.3.12.2 Cada servidor é administrado individualmente - as políticas são gerenciadas localmente, mas a Política pai padrão é herdada do servidor superior

A configuração do cenário anterior também se aplica a esse cenário. No entanto, o servidor A tem a política padrão para servidores inferiores habilitada, e as políticas nos servidores inferiores herdam a configuração da política pai padrão do servidor mestre. Nesse cenário, os administradores locais têm um alto grau de autonomia para configurar políticas. Embora as políticas filha nos servidores inferiores podem herdar a política pai padrão, os administradores locais ainda podem modificá-la por suas próprias políticas.



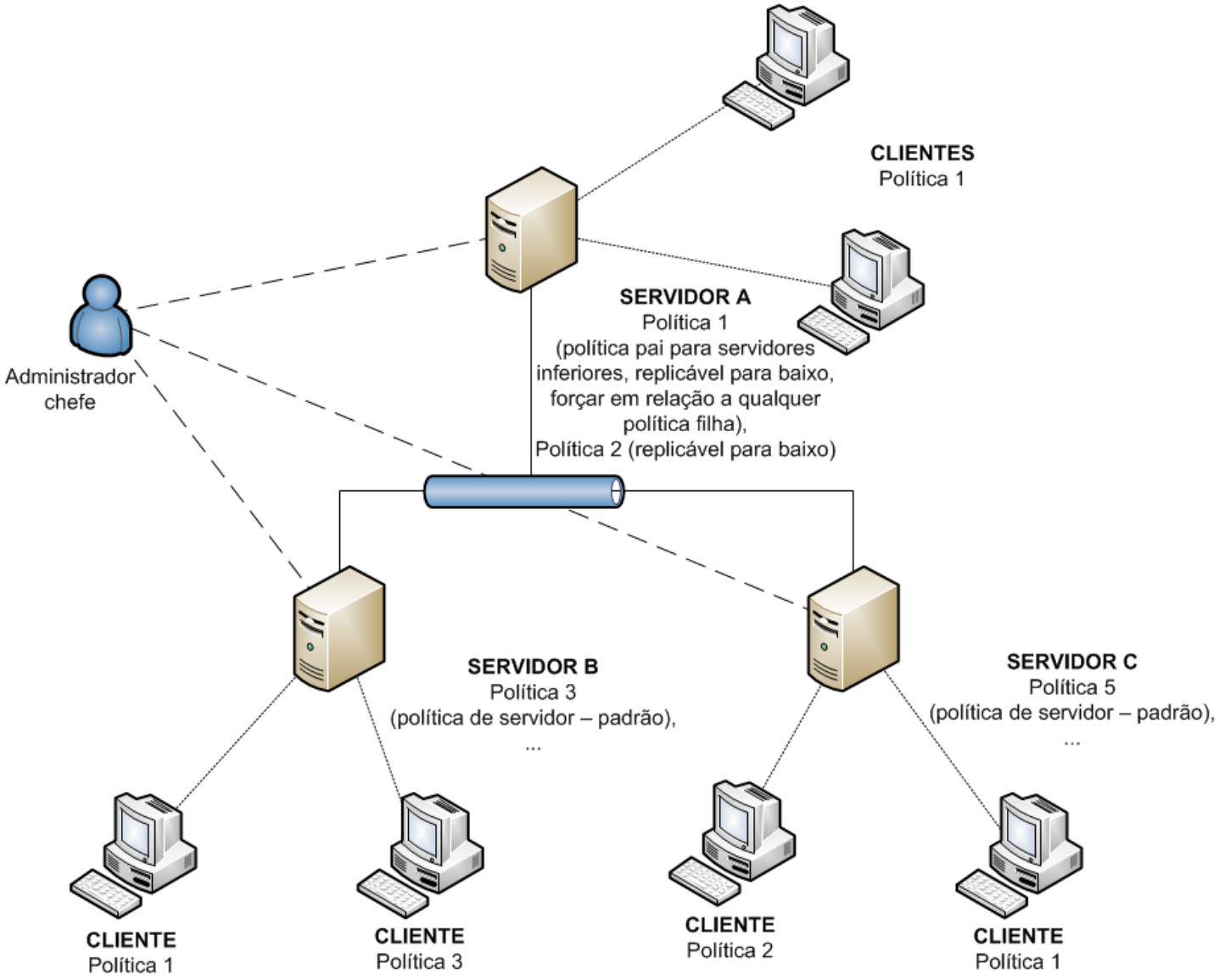
5.3.12.3 Herdando políticas de um servidor superior

O modelo de rede para esse cenário é o mesmo que para os dois cenários anteriores. Além disso, o servidor mestre, junto com a Política pai padrão, contém outras políticas, que são replicáveis para baixo e servem como políticas pai nos servidores inferiores. Para a Política 1 (veja a figura a seguir), o atributo **Substituir qualquer política filha** está ativado. O administrador local ainda terá um grande grau de autonomia, mas o administrador principal define quais políticas são replicadas para baixo e quais delas servem como políticas pai para políticas locais. O atributo **Substituir...** define que configurações definidas nas políticas selecionadas substituem aquelas definidas nos servidores locais.



5.3.12.4 Atribuindo políticas somente do servidor superior

Este cenário representa um sistema centralizado do gerenciamento de políticas. Políticas para clientes são criadas, modificadas e atribuídas somente no servidor principal - o administrador local não tem direitos para modificá-las. Todos os servidores inferiores têm somente uma política básica, que está vazia (por padrão, intitulada Política do servidor). Essa política serve como a Política pai padrão para clientes primários.



5.3.12.5 Usando grupos

Em algumas situações, atribuir políticas a grupos de clientes pode complementar cenários anteriores. Os grupos podem ser criados manualmente ou usando a opção **Sincronização do Active Directory**.

Clientes podem ser adicionados a grupos manualmente (**Grupos estáticos**) ou automaticamente - pelas propriedades de grupo (**Grupos paramétricos**). Consulte o capítulo Gerenciador de grupos 69 para obter mais detalhes.

Para atribuir uma política a um grupo de clientes, você pode usar a opção de atribuição individual em **Gerenciador de políticas** (**Adicionar clientes > Adicionar especial**) ou fornecer políticas automaticamente via **Regras de política**.

Um dos possíveis cenários é o seguinte:

O administrador quer atribuir diferentes políticas para clientes pertencendo a diferentes grupos do AD, bem como alterar a política do cliente automaticamente quando o cliente for movido para outro grupo do AD.

1) A primeira etapa é definir a **Sincronização do Active Directory** no **Gerenciador de grupos** de acordo com suas necessidades. O importante aqui é agendar devidamente a sincronização do AD (possíveis opções: por hora, diariamente, semanalmente, mensalmente).

2) Depois da primeira sincronização bem-sucedida, os grupos do AD aparecem na seção **Grupos estáticos**.

3) Crie uma nova regra de política e marque **Grupos do ERA EM** e/ou **Grupos do ERA NÃO EM** como uma condição de regra.

4) Especifique os grupos do AD que você deseja adicionar à condição.

5) Na próxima etapa, defina a política que será aplicada a clientes correspondendo às condições de regra e pressione **OK** para salvar a regra.

OBSERVAÇÃO: As etapas 3 a 5 podem ser substituídas usando o **Assistente de regras de política**, que permite que você crie uma estrutura de política com base na estrutura de grupo existente, bem como que você mapeie políticas criadas para grupos ao criar regras de política correspondentes.

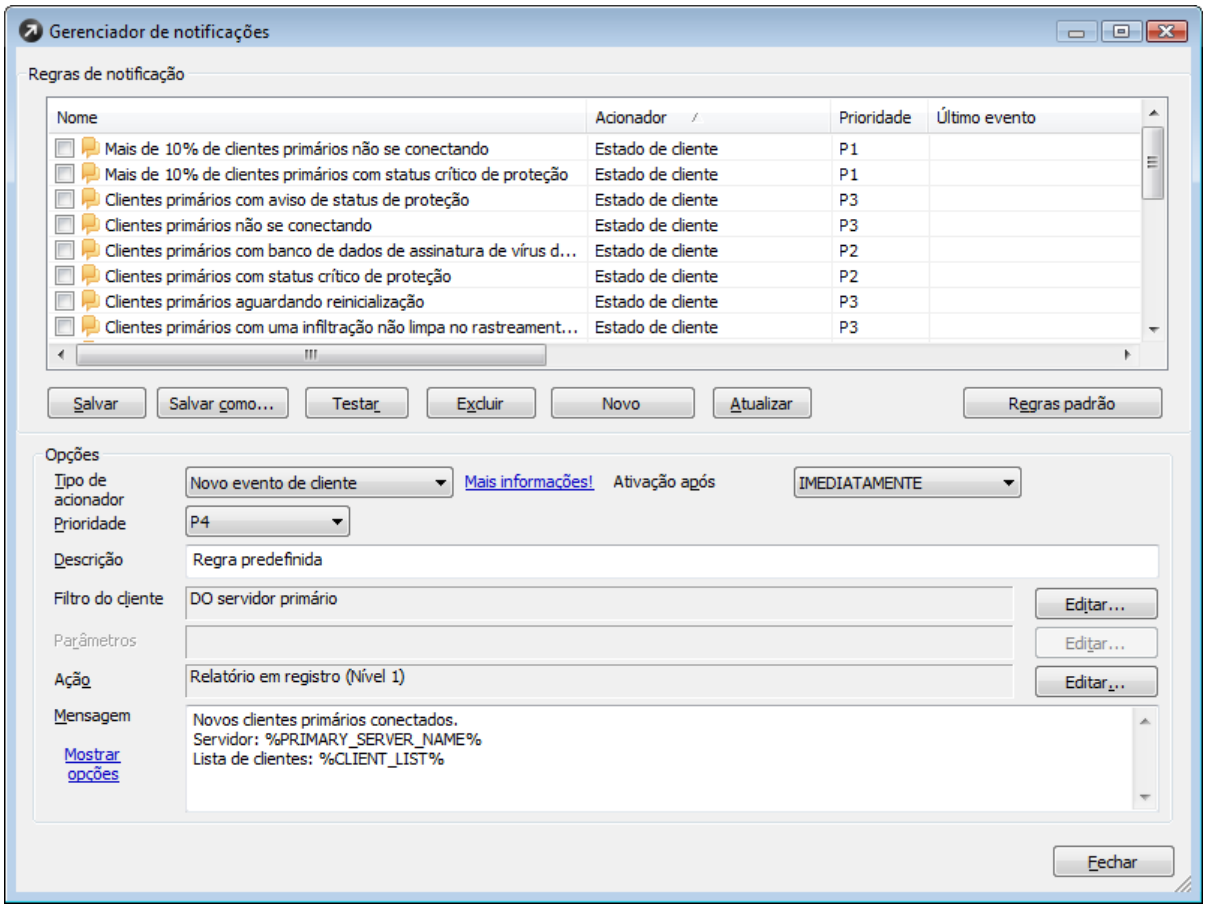
Dessa forma, é possível definir uma regra de política específica para cada grupo do AD. Atribuir uma determinada política a um cliente específico agora depende da associação do cliente em um grupo do AD específico. Como a sincronização do AD está agendada para ocorrer regularmente, todas as alterações na associação dos grupos do AD do cliente serão atualizadas e consideradas quando uma regra de política for aplicada. Em outras palavras, políticas são aplicadas a clientes automaticamente, dependendo de seu grupo do AD. Assim que as regras e políticas forem totalmente definidas, não será necessária mais nenhuma intervenção do administrador em relação à aplicação da política.

A principal vantagem dessa abordagem é um vínculo direto e automático entre a associação do grupo do AD e a atribuição de política.

5.4 Gerenciador de notificações

A capacidade de notificar os administradores de rede e do sistema sobre eventos importantes é um aspecto essencial da integridade e segurança da rede. Um aviso antecipado sobre um erro ou código malicioso pode impedir a enorme perda de tempo e dinheiro frequentemente necessários para eliminar tais problemas posteriormente. As próximas três seções descrevem as opções de notificação oferecidas pelo ERA.

Para abrir a janela principal **Gerenciador de notificações**, clique em **Ferramentas** > **Gerenciador de notificações**.



A janela principal é dividida em duas seções:

1. A seção **Regras de notificação** na parte superior da janela contém uma lista de regras existentes (predefinidas ou definidas pelo usuário). Uma regra nessa seção deve ser selecionada para gerar mensagens de notificação. Por padrão, está habilitada a opção sem notificações. Portanto, recomendamos verificar se suas regras estão ativas. Os

botões funcionais na lista de regras incluem **Salvar** (salvar modificações em uma regra), **Salvar como...** (salvar modificações em uma regra com um novo nome), **Excluir**, **Testar** (clicar neste botão acionará imediatamente a regra e enviará uma notificação), **Novo** (use este botão para criar novas regras), **Atualizar** e **Regras padrão** (atualize a lista com regras padrão).

Por padrão, a janela **Gerenciador de notificações** contém regras predefinidas. Para ativar uma regra, marque a caixa de seleção ao lado da regra. As regras de notificação a seguir estão disponíveis. Se elas forem ativadas e as condições de regra atendidas, elas gerarão entradas de log.

- **Mais de 10% de clientes primários não se conectando** - se mais de 10% de clientes não tiverem se conectado ao servidor por mais de uma semana; a regra será executada URGENTE se esse for o caso.
- **Mais de 10% de clientes primários com status crítico de proteção** - se mais de 10% de clientes tiverem gerado um aviso de status crítico e não tiverem se conectado ao servidor por mais de uma semana; a regra será executada URGENTE se esse for o caso.
- **Clientes primários com aviso de status de proteção** - se houver pelo menos um cliente com um aviso de status de proteção que não tiver se conectado ao servidor por, pelo menos, uma semana.
- **Clientes primários não se conectando** - se houver pelo menos um cliente que não tiver se conectado ao servidor por mais de uma semana.
- **Clientes primários com banco de dados de assinatura de vírus desatualizado** - se houver um cliente com um banco de dados de assinatura de vírus duas ou mais versões anteriores à atual e não tiver sido desconectado do servidor por mais de uma semana.
- **Clientes primários com status crítico de proteção** - se houver um cliente com um aviso de status de proteção crítico que não tiver se desconectado por mais de uma semana.
- **Clientes primários com banco de dados de assinatura de vírus mais recente do que o do servidor** - se houver um cliente com um banco de dados de assinatura de vírus mais recente do que o do servidor e não tiver sido desconectado por mais de uma semana.
- **Clientes primários aguardando reinicialização** - se houver um cliente aguardando reinicialização que não tiver sido desconectado por mais de uma semana.
- **Clientes primários com uma infiltração não limpa no rastreamento do computador** - se houver um cliente no qual um rastreamento de computador não possa ter sido possível limpar pelo menos uma infiltração, bem como esse cliente não tenha sido desconectado por mais de uma semana; a regra será executada URGENTE se esse for o caso.
- **Tarefa concluída** - se houver uma tarefa concluída em um cliente; a regra será executada URGENTE se esse for o caso.
- **Novos clientes primários** - se um novo cliente tiver se conectado ao servidor; a regra será executada URGENTE se esse for o caso.
- **Novos clientes replicados** - se houver um novo cliente replicado na lista de clientes; a regra será executada depois de uma hora se esse for o caso.
- **Possível epidemia de vírus** - se a frequência de entradas de log de ameaça em um cliente tiver excedido 1.000 avisos críticos em uma hora em, pelo menos, 10% de todos os clientes.
- **Possível ataque de rede** - se a frequência de entradas de log do ESET Personal Firewall em um cliente tiver excedido 1.000 avisos críticos em uma hora em, pelo menos, 10% de todos os clientes.
- **Servidor atualizado** - se o servidor tiver sido atualizado.
- **Servidor não atualizado** - se o servidor não tiver sido atualizado por mais de cinco dias; a regra será executada URGENTE se esse for o caso.
- **Erro em log de texto de servidor** - se o log de servidor tiver uma entrada de erro.
- **Expiração de licença** - se a licença atual expirar em 20 dias e após a expiração, o número máximo de licenças de cliente será inferior ao número atual de clientes; a regra será executada URGENTE se esse for o caso.
- **Limite de licença** - se o número de licenças de clientes livres ficar abaixo de 10% de todas as licenças de clientes disponíveis.

Se não houver declaração contrária, todas as regras serão executadas e repetidas depois de 24 horas e aplicadas ao servidor primário e a clientes primários.

2. A seção **Opções** na metade inferior da janela fornece informações sobre a regra atualmente selecionada. Todos os campos e opções nesta seção são descritos usando a regra de exemplo do capítulo Criação de regras 90.

Em cada regra, você pode especificar os critérios, conhecidos como um **Acionador**, que ativa a regra. Os seguintes acionadores estão disponíveis:

- Estado de cliente 84 - a regra será executada se houver um problema em alguns dos clientes.
- Estado de servidor 86 - a regra será executada se houver um problema em alguns dos servidores.
- Evento de tarefa concluído 87 - a regra será executada depois que a tarefa especificada for concluída.

- Novo evento de cliente 87 - a regra será executada se houver um novo cliente se conectando ao servidor (incluindo clientes replicados).
- Evento de epidemia 88 - a regra será executada se houver uma epidemia de incidentes em uma quantidade significativa de clientes.
- Evento de log recebido 88 - a regra será executada no caso de o administrador desejar ser notificado sobre os logs em determinado intervalo de tempo.

Com base no tipo de acionador, outras opções de regra poderão ser ativadas ou desativadas; portanto, recomendamos definir o tipo de acionador primeiro ao criar novas regras 90.

O menu suspenso **Prioridade** permite selecionar prioridade de regra. **P1** é a prioridade mais alta, **P5** é a prioridade mais baixa. A prioridade não afeta de forma alguma a funcionalidade de regras. Para atribuir prioridade a mensagens de notificação, a variável *%PRIORITY%* poderá ser usada. No menu suspenso **Prioridade**, há um campo **Descrição**. Recomendamos que cada regra receba uma descrição significativa, como *"regra que avisa sobre infiltrações detectadas"*.

O formato de notificação pode ser editado no campo **Mensagem**, na seção inferior da janela principal do Gerenciador de notificações. No texto, você pode usar variáveis especiais *%VARIABLE_NAME%*. Para ver a lista de variáveis disponíveis, clique em **Mostrar-me opções**.

- **Rule_Name**
- **Rule_Description**
- **Prioridade** - prioridade da regra de notificação (P1 tem a mais alta prioridade).
- **Acionada** - data da notificação mais recente enviada (repetições excluídas).
- **Triggered_Last** - data da notificação mais recente enviada (repetições incluídas).
- **Client_Filter** - parâmetros de filtro do cliente.
- **Client_Filter_Short** - configurações de filtro do cliente (em forma abreviada).
- **Client_List** - lista de clientes.
- **Parâmetros** - parâmetros de regra.
- **Primary_Server_Name**
- **Server_Last_Updated** - última atualização do servidor.
- **Virus_Signature_DB_Version** - versão mais recente do banco de dados de assinatura de vírus.
- **Pcu_List** - lista mais recente de todos os PCUs.
- **Pcu_List_New_Eula** - lista mais recente de todos os PCUs com um novo EULA.
- **Last_Log_Date** - data do último log.
- **Task_Result_List** - lista de tarefas concluídas.
- **Log_Text_Truncated** - texto de log que ativou a notificação (truncado).
- **License_Info_Merged** - informações de licença (resumo).
- **License_Info_Full** - informações de licença (completas).
- **License_Days_To_Expiry** - dias restantes até a expiração da licença.
- **License_Expiration_Date** - data de expiração mais próxima.
- **License_Clients_Left** - licenças livres na licença atual para clientes se conectarem ao servidor.
- **Actual_License_Count** - número de clientes atualmente conectados ao servidor.

5.4.1 Estado de cliente

Defina os parâmetros de filtragem do cliente na janela **Filtro do cliente**. Quando uma regra for aplicada, somente clientes atendendo aos critérios de filtro do cliente serão considerados. Os critérios de filtragem são:

- **DO servidor primário** - somente clientes do servidor primário (a negativa NÃO DO também pode ser aplicada).
- **Servidor primário incluído** - inclui o servidor primário na saída.
- **TEM sinalizador Novo** - clientes marcados pelo sinalizador *"Novo"* (a negativa NÃO TEM também pode ser aplicada).
- **Grupos do ERA incluídos** - clientes pertencendo ao grupo especificado.
- **Domínio/grupo de trabalho incluído** - clientes pertencendo ao domínio especificado.
- **Máscara de nome de computador** - clientes com o nome de computador especificado.
- **TEM máscara IPv4** - clientes que se encaixam na máscara IPv4 especificada.
- **TEM intervalo IPv4** - clientes no intervalo de endereços IPv4 especificado.
- **TEM prefixo de rede IPv6** - clientes no prefixo de rede IPv6 especificado.
- **TEM intervalo IPv6** - clientes no intervalo de endereços IPv6 especificado.
- **TEM política definida** - clientes com a política especificada atribuída (a negativa NÃO TEM também pode ser

aplicada).

Depois que você tiver especificado um filtro de cliente para sua regra de notificação, clique em **OK** e proceda para os parâmetros de regra. Os parâmetros do cliente definem qual condição um cliente ou grupo de clientes deve atender para executar a ação de notificação. Para visualizar o parâmetro disponível, clique no botão **Editar...** na seção **Parâmetros**.

A disponibilidade de parâmetros depende do tipo de acionador selecionado. Os seguintes parâmetros estão disponíveis para acionadores do estado do cliente:

- **Quaisquer avisos de status de proteção** - qualquer aviso encontrado na coluna Status de proteção.
- **Avisos críticos de status de proteção** - qualquer aviso crítico encontrado na coluna Status de proteção.
- **Versão do banco de dados de assinatura de vírus** - problema com o banco de dados de assinatura de vírus (6 valores possíveis):

  - **Anterior** - o banco de dados de assinatura de vírus é uma versão anterior à atual.
  - **Anterior ou N/D** - o banco de dados de assinatura de vírus é mais de uma versão anterior à atual.
  - **Anterior a 5 versões ou N/D** - o banco de dados de assinatura de vírus é mais de 5 versões anteriores à atual.
  - **Anterior a 10 versões ou N/D** - o banco de dados de assinatura de vírus é mais de 10 versões anteriores à atual.
  - **Anterior a 7 dias ou N/D** - o banco de dados de assinatura de vírus é mais de 7 dias anteriores à atual.
  - **Anterior a 14 dias ou N/D** - o banco de dados de assinatura de vírus é mais de 14 dias anteriores à atual.

- **Aviso de última conexão** - a última conexão foi estabelecida antes do período de tempo especificado.
- **Tem último evento de ameaça** - a coluna Ameaça contém um aviso de ameaça.
- **Tem último evento** - a coluna Último evento contém uma entrada.
- **Tem último evento de firewall** - a coluna Evento de firewall contém uma entrada de evento de firewall.
- **Tem sinalizador Novo** - o cliente tem o sinalizador "Novo".
- **Aguardando reinicialização** - o cliente está aguardando reinicialização.
- **Último rastreamento detectou ameaça** - no cliente, o número especificado de ameaças foi encontrado durante o último rastreamento.
- **Último rastreamento não limpou ameaça** - no cliente, o número especificado de ameaças não limpas foi encontrado durante o último rastreamento.

Todos os parâmetros podem ser negados, mas todas as negações serão utilizáveis. Somente é adequado negar os parâmetros que incluam dois valores lógicos: verdadeiro e não verdadeiro. Por exemplo, o parâmetro **Tem sinalizador Novo** cobre somente clientes com o sinalizador *"Novo"*. O parâmetro negativo incluiria todos os clientes não marcados pelo sinalizador.

Todas as condições acima podem ser logicamente combinadas e invertidas. O menu suspenso **A regra é aplicada quando** oferece duas opções:

- **todas as opções são atendidas** - a regra será executada somente se **todos** os parâmetros especificados forem atendidos.
- **qualquer uma das opções é atendida** - a regra será executada se, pelo menos, **uma** condição for atendida.

Se os parâmetros especificados para uma regra forem atendidos, a ação definida pelo administrador será automaticamente realizada. Para configurar ações, clique em **Editar...** na seção Ação 89.

A ativação da regra pode ser adiada por um período de tempo variando de uma hora a três meses. Se você quiser ativar a regra assim que possível, selecione **URGENTE** no menu suspenso **Ativação após**. O Gerenciador de notificações é ativado a cada 10 minutos por padrão, então se você selecionar **URGENTE**, a tarefa deve ser executada em 10 minutos. Se um período de tempo específico for selecionado a partir desse menu, a ação será automaticamente realizada depois que o período de tempo tiver sido decorrido (desde que a condição de regra seja atendida).

O menu **Repetir a cada...** permite que você especifique um intervalo de tempo após o qual a ação será repetida. No entanto, a condição para ativar a regra ainda deverá ser atendida. Em **Servidor** > **Avançadas** > **Editar configurações avançadas** > **ESET Remote Administrator** > **Servidor** > **Configuração** > **Notificações** > **Intervalo para processamento de notificação (minutos)**, você poderá especificar o intervalo de tempo no qual o servidor verificará e executará regras ativas.

O valor padrão é de 10 minutos. Não recomendamos diminuí-lo, pois isso poderá causar lentidão significativa no servidor.

5.4.2 Estado de servidor

A janela **Parâmetros de regra do servidor** permite que você configure parâmetros para acionar uma regra relacionada ao estado específico, que é então aplicada ao envio de notificações. Para configurar um parâmetro, clique no botão de opção ao lado de uma condição específica. Isso ativará os elementos ativos adjacentes da GUI, a fim de permitir que você modifique os parâmetros de uma condição.

- **Servidor atualizado** - o servidor está atualizado.
- **Servidor não atualizado** - o servidor não está atualizado por mais tempo do que o especificado.
- **Log de auditoria** - o **Log de auditoria** monitora e registra em log todas as alterações na configuração e ações realizadas por todos os usuários do ERAC. Você pode filtrar as entradas de log por tipo, consulte **Log de servidor**.
- **Log de servidor** - o log de servidor contém os seguintes tipos de entrada:

  - **Erros** - mensagens de erro

  - **Erros+Avisos** - mensagens de erro e mensagens de aviso

  - **Erros+Avisos+Informações (detalhamento)** - mensagens de erro, de aviso e informativas

  - **Filtrar entradas de log por tipo** - habilite esta opção para especificar entradas de aviso e erro a serem observadas no log do servidor. Observe que para que as notificações funcionem devidamente, o detalhamento de log (**Ferramentas > Opções do servidor > Registro em log**) deve ser definido para o nível correspondente. Caso contrário, tais regras de notificação nunca localizarão um acionador no log de servidor. As seguintes entradas de log estão disponíveis:

- **ADSI_SYNCHRONIZE** - sincronização do grupo do Active Directory.
- **CLEANUP** - tarefas de limpeza do servidor.
- **CREATEREPORT** - geração de relatório sob demanda.
- **DEINIT** - desligamento do servidor.
- **INIT** - inicialização do servidor.
- **INTERNAL 1** - mensagem de servidor interno.
- **INTERNAL 2** - mensagem de servidor interno.
- **LICENSE** - administração de licença.
- **MAINTENANCE** - tarefas de manutenção do servidor.
- **NOTIFICATION** - gerenciamento de notificações.
- **PUSHINST** - instalação forçada.
- **RENAME** - para renomear a estrutura interna.
- **REPLICATION** - replicação do servidor.
- **POLICY** - gerenciamento de políticas.
- **POLICYRULES** - regras de política.
- **SCHEDREPORT** - relatórios gerados automaticamente.
- **SERVERMGR** - gerenciamento de encadeamentos do servidor interno.
- **SESSION** - conexões de rede do servidor.
- **SESSION_USERACTION** - várias ações do usuário.
- **THREATSENSE** - ESET Live Grid - envio de informações estatísticas.
- **UPDATER** - criação de imagem e atualização do servidor.

Um exemplo de um parâmetro útil é o UPDATER, que envia uma mensagem de notificação quando o Gerenciador de notificações localiza um problema relacionado à criação de imagem e à atualização nos logs de servidor.

- **Expiração de licença** - a licença expirará no número especificado de dias ou já expirou. Selecione **Avisar somente se isso fizer com que o número de clientes na licença fique abaixo do número de clientes reais no banco de dados do servidor** para enviar uma notificação se a expiração for fazer com que o número de licenças na licença fique abaixo do número de clientes atualmente conectados.
- **Limitar licença** - se o percentual de clientes livres estiver abaixo do valor especificado.

Se os parâmetros especificados para uma regra forem atendidos, a ação definida pelo administrador será automaticamente realizada. Para configurar ações, clique em **Editar...** na seção Ação 89.

A ativação da regra pode ser adiada por um período de tempo variando de uma hora a três meses. Se você quiser ativar a regra assim que possível, selecione **URGENTE** no menu suspenso **Ativação após**. O Gerenciador de notificações é ativado a cada 10 minutos por padrão, então se você selecionar **URGENTE**, a tarefa deve ser executada em 10 minutos. Se um período de tempo específico for selecionado a partir desse menu, a ação será automaticamente realizada depois que o período de tempo tiver sido decorrido (desde que a condição de regra seja atendida).

O menu **Repetir a cada...** permite que você especifique um intervalo de tempo após o qual a ação será repetida. No entanto, a condição para ativar a regra ainda deverá ser atendida. Em **Servidor** > **Avançadas** > **Editar configurações avançadas** > **ESET Remote Administrator** > **Servidor** > **Configuração** > **Notificações** > **Intervalo para processamento de notificação (minutos)**, você poderá especificar o intervalo de tempo no qual o servidor verificará e executará regras ativas.

O valor padrão é de 10 minutos. Não recomendamos diminuí-lo, pois isso poderá causar lentidão significativa no servidor.

5.4.3 Evento de tarefa concluído

A regra será acionada depois que as tarefas selecionadas forem concluídas. Em configurações **padrão**, todos os tipos de tarefa 64 serão selecionados.

Se os parâmetros especificados para uma regra forem atendidos, a ação definida pelo administrador será automaticamente realizada. Para configurar ações, clique em **Editar...** na seção Ação 89.

A ativação da regra pode ser adiada por um período de tempo variando de uma hora a três meses. Se você quiser ativar a regra assim que possível, selecione URGENTE no menu suspenso **Ativação após**. O Gerenciador de notificações é ativado a cada 10 minutos por padrão, então se você selecionar **URGENTE**, a tarefa deve ser executada em 10 minutos. Se um período de tempo específico for selecionado a partir desse menu, a ação será automaticamente realizada depois que o período de tempo tiver sido decorrido (desde que a condição de regra seja atendida).

5.4.4 Novo evento de cliente

Defina os parâmetros de filtragem do novo cliente na janela **Filtro do cliente**. Quando uma regra for aplicada, somente clientes atendendo aos critérios de filtro do cliente serão considerados. Os critérios de filtragem são:

- **DO servidor primário** - somente clientes do servidor primário (a negativa NÃO DO também pode ser aplicada).
- **Servidor primário incluído** - inclui o servidor primário na saída.
- **TEM novo sinalizador** - clientes marcados pelo sinalizador *"Novo"* (a negativa NÃO TEM também pode ser aplicada).
- **Grupos do ERA incluídos** - clientes pertencendo ao grupo especificado.
- **Domínio/grupo de trabalho incluído** - clientes pertencendo ao domínio especificado.
- **Máscara de nome de computador** - clientes com o nome de computador especificado.
- **TEM máscara IPv4** - clientes que se encaixam na máscara IPv4 especificada.
- **TEM intervalo IPv4** - clientes no intervalo de endereços IPv4 especificado.
- **TEM prefixo de rede IPv6** - clientes no intervalo de endereços IPv6 especificado.
- **TEM intervalo IPv6** - clientes no intervalo de endereços IPv6 especificado.
- **TEM política definida** - clientes com a política especificada atribuída (a negativa NÃO TEM também pode ser aplicada).

Se os parâmetros especificados para uma regra forem atendidos, a ação definida pelo administrador será automaticamente realizada. Para configurar ações, clique em **Editar...** na seção Ação 89.

A ativação da regra pode ser adiada por um período de tempo variando de uma hora a três meses. Se você quiser ativar a regra assim que possível, selecione **URGENTE** no menu suspenso **Ativação após**. O Gerenciador de notificações é ativado a cada 10 minutos por padrão, então se você selecionar **URGENTE**, a tarefa deve ser executada em 10 minutos. Se um período de tempo específico for selecionado a partir desse menu, a ação será automaticamente realizada depois que o período de tempo tiver sido decorrido (desde que a condição de regra seja atendida).

5.4.5 Evento de epidemia

Esta notificação será acionada assim que os critérios definidos para uma epidemia de incidentes forem atendidos; ela não reportará cada incidente individual ou incidentes excedendo os critérios definidos.

Defina os parâmetros de filtragem para um evento de epidemia na janela **Filtro do cliente**. Quando uma regra for aplicada, somente clientes atendendo aos critérios de filtro do cliente serão considerados. Os critérios de filtragem são:

- **DO servidor primário** - somente clientes do servidor primário (a negativa NÃO DO também pode ser aplicada).
- **Servidor primário incluído** - inclui o servidor primário na saída.
- **TEM novo sinalizador** - clientes marcados pelo sinalizador *"Novo"* (a negativa NÃO TEM também pode ser aplicada).
- **Grupos do ERA incluídos** - clientes pertencendo ao grupo especificado.
- **Domínio/grupo de trabalho incluído** - clientes pertencendo ao domínio especificado.
- **Máscara de nome de computador** - clientes com o nome de computador especificado.
- **TEM máscara IPv4** - clientes que se encaixam na máscara IPv4 especificada.
- **TEM intervalo IPv4** - clientes no intervalo de endereços IPv4 especificado.
- **TEM prefixo de rede IPv6** - clientes no intervalo de endereços IPv6 especificado.
- **TEM intervalo IPv6** - clientes no intervalo de endereços IPv6 especificado.
- **TEM política definida** - clientes com a política especificada atribuída (a negativa NÃO TEM também pode ser aplicada).

Depois que você tiver especificado um filtro de cliente para sua regra de notificação, clique em **OK** e proceda para os parâmetros de regra. Os parâmetros do cliente definem qual condição um cliente ou grupo de clientes deve atender para executar a ação de notificação. Para visualizar o parâmetro disponível, clique no botão **Editar...** na seção **Parâmetros**.

- **Tipo de log** - selecione o tipo do log que deseja monitorar.
- **Nível de log** - nível de entrada de log no log especificado.
  - Nível 1 - Avisos críticos - somente erros críticos.
  - Nível 2 - Acima + Avisos - o mesmo que 1, mais notificações de alerta.
  - Nível 3 - Acima + Normal - o mesmo que 2, mais notificações informativas.
  - Nível 4 - Acima + Diagnóstico - o mesmo que 3, mais notificações diagnósticas.
- **1.000 ocorrências em 60 minutos** - digite o número de ocorrências e selecione o período de tempo para especificar a frequência de eventos que deve ser atingida para a notificação ser enviada. A frequência padrão é de 1.000 ocorrências em uma hora.
- **Quantidade** - número de clientes (absoluto ou em percentual).

O **Intervalo de alternância** é o intervalo de tempo usado para enviar as notificações. Por exemplo, se o intervalo de alternância for definido como 1 hora, os dados serão coletados em segundo plano e você receberá a notificação a cada hora (no caso de haver uma epidemia e o acionador estar ativo).

5.4.6 Evento de log recebido

Esta opção será usada quando você quiser ser notificado sobre cada log em determinado intervalo de tempo.

Defina os parâmetros de filtragem do cliente na janela **Filtro do cliente**. Quando uma regra for aplicada, somente clientes atendendo aos critérios de filtro do cliente serão considerados. Os critérios de filtragem são:

- **DO servidor primário** - somente clientes do servidor primário (a negativa NÃO DO também pode ser aplicada).
- **Servidor primário incluído** - inclui o servidor primário na saída.
- **TEM novo sinalizador** - clientes marcados pelo sinalizador *"Novo"* (a negativa NÃO TEM também pode ser aplicada).
- **Grupos do ERA incluídos** - clientes pertencendo ao grupo especificado.
- **Domínio/grupo de trabalho incluído** - clientes pertencendo ao domínio especificado.

- **Máscara de nome de computador** - clientes com o nome de computador especificado.
- **TEM máscara IPv4** - clientes que se encaixam na máscara IPv4 especificada.
- **TEM intervalo IPv4** - clientes no intervalo de endereços IPv4 especificado.
- **TEM prefixo de rede IPv6** - clientes no intervalo de endereços IPv6 especificado.
- **TEM intervalo IPv6** - clientes no intervalo de endereços IPv6 especificado.
- **TEM política definida** - clientes com a política especificada atribuída (a negativa NÃO TEM também pode ser aplicada).

Depois que você tiver especificado um filtro de cliente para sua regra de notificação, clique em **OK** e proceda para os parâmetros de regra. Os parâmetros do cliente definem qual condição um cliente ou grupo de clientes deve atender para executar a ação de notificação. Para visualizar o parâmetro disponível, clique no botão **Editar...** na seção **Parâmetros**.

- **Tipo de log** - selecione o tipo do log que deseja monitorar.
- **Nível de log** - nível de entrada de log no log especificado.
  - Nível 1 - Avisos críticos - somente erros críticos.
  - Nível 2 - Acima + Avisos - o mesmo que 1, mais notificações de alerta.
  - Nível 3 - Acima + Normal - o mesmo que 2, mais notificações informativas.
  - Nível 4 - Acima + Diagnóstico - o mesmo que 3, mais notificações diagnósticas.

Se os parâmetros especificados para uma regra forem atendidos, a ação definida pelo administrador será automaticamente realizada. Para configurar ações, clique em **Editar...** na seção Ação 89.

O **Intervalo de alternância** é o intervalo de tempo usado para enviar as notificações. Por exemplo, se o intervalo de alternância for definido como 1 hora, os dados serão coletados em segundo plano e você receberá a notificação a cada hora (no caso de o acionador ainda estar ativo).

5.4.7 Ação

Se os parâmetros especificados para uma regra forem atendidos, a ação definida pelo administrador será automaticamente realizada. Para configurar ações, clique em **Editar...** na seção **Ações**. O editor de ações oferece estas opções:

- **Email** - o programa envia o texto de notificação da regra para o endereço de email especificado; no **Assunto**, você pode especificar o assunto. Clique em **Para** para abrir o catálogo de endereços.
- **Interceptação SNMP** - gera e envia notificações SNMP.
- **Executar (no servidor)** - habilita essa opção e especifica o aplicativo para ser executado no servidor. Informe o caminho completo do aplicativo.
- **Registrar em arquivo** - gera entradas de log no arquivo de log especificado. Informe o caminho completo para a pasta; o **Detalhamento** de notificações pode ser configurado.
- **Registrar no Syslog** - registre notificações nos logs do sistema; o **Detalhamento** de notificações pode ser configurado.
- **Registro em log** - registra notificações nos logs do sistema; o **Detalhamento** de notificações pode ser configurado.
- **Executar relatório** - depois de selecionar essa opção, o menu suspenso **Nome do modelo** se tornará clicável. Aqui, selecione um modelo que você deseja usar para o relatório. Para obter mais informações sobre os modelos, consulte o capítulo Relatórios 36.

Para que esse recurso funcione corretamente, você deve habilitar o registro em log no ERA Server (**Ferramentas** > **Opções do servidor** > **Registro em log**).

5.4.8 Notificações via Interceptação SNMP

O SNMP (Simple Network Management Protocol, Protocolo de gerenciamento de rede simples) é um protocolo de gerenciamento simples e abrangente, que é adequado para o monitoramento e a identificação de problemas de rede. Uma das operações desse protocolo é a interceptação, que envia dados específicos. No ERA, usamos a interceptação para enviar mensagens de notificação.

Para que a ferramenta de interceptação seja executada efetivamente, o protocolo SNMP deve ser corretamente instalado e configurado no mesmo computador que o ERAS (**Iniciar** > **Painel de controle** > **Adicionar ou remover programas** > **Adicionar/remover componentes do Windows**). O serviço SNMP deve ser configurado como descrito neste artigo: http://support.microsoft.com/kb/315154. No ERAS, você precisa ativar uma regra de notificação de SNMP.

As notificações podem ser visualizados no gerenciador de SNMP, que deve ser conectado a um servidor de SNMP, no qual o arquivo de configuração *eset_ras.mib* tenha sido importado. O arquivo é um componente padrão de uma instalação do ERA e geralmente está localizado na pasta C:*Program Files**ESET**ESET Remote Administrator**Server**snmp*\.

5.4.9 Exemplo de criação de regras

As etapas a seguir demonstram como criar uma regra que enviará uma notificação por e-mail para o administrador se houver um problema com o Status de proteção de qualquer uma das estações de trabalho clientes. A notificação também será salva em um arquivo nomeado *log.txt*.

1) Defina o menu suspenso **Tipo de acionador** como **Estado de cliente**.

2) Deixe as opções **Prioridade, Ativação após:** e **Repetir depois de cada:** nos valores predefinidos. A regra receberá automaticamente a prioridade 3 e será desativada depois de 24 horas.

3) No campo **Descrição**, digite **notificação do status de proteção para clientes no grupo da sede**.

4) Clique em **Editar...** na seção **Filtro do cliente** e ative somente a condição de regra da seção **Grupos ERA INSERIDOS** . Na parte inferior dessa janela, clique no link **especificar** e digite *Sede* na nova janela. Clique em **Adicionar** e clique em **OK** (duas vezes) para confirmar. Isso designa que a regra será aplicada somente a clientes do grupo da sede.

5) Especifique mais parâmetros para a regra em **Parâmetros > Editar...**. Desmarque todas as opções, exceto **Quaisquer avisos de status de proteção**.

6) Vá para a seção **Ação** e clique no botão **Editar...**. Na janela **Ação**, ative **Email**, especifique destinatários (**Para...**) e **Assunto** para o email. Em seguida, marque a caixa de seleção **Registrar em arquivo**, e insira o nome e caminho do arquivo de log a ser criado. Como uma opção, você pode selecionar o **Detalhamento** do arquivo de log. Clique em **OK** para salvar a ação.

7) Por fim, use a área de texto **Mensagem** para especificar o detalhamento que será enviado no corpo do email quando a regra for ativada. Exemplo: *"O cliente %CLIENT_LIST% reporta problema no status de proteção"*.

8) Clique em **Salvar como...** para nomear a regra, p. ex., *"problemas no status de proteção"* e selecione a regra na lista de regras de notificação.

A regra agora está ativa. Se houver um problema com o status de proteção em um cliente do grupo da sede, a regra será executada. O administrador receberá uma notificação por e-mail com um anexo contendo o nome do cliente problemático. Clique em **Fechar** para sair do Gerenciador de notificações.

5.5 Informações detalhadas de clientes

O ERA permite que você extraia informações sobre processos em execução, programas de inicialização, etc. de estações de trabalho clientes. Essas informações podem ser recuperadas usando a ferramenta ESET SysInspector integrada, que é integrada diretamente com o ERAS. Junto com outras funções úteis, o ESET SysInspector examina totalmente o sistema operacional e cria logs de sistema. Para abri-lo, clique em **Ferramentas** > **ESET SysInspector** no menu principal do ERAC.
Se houver problemas com um cliente específico, você pode solicitar um log do ESET SysInspector desse cliente. Para fazer isso, clique com o botão direito do mouse no cliente no painel **Clientes** e selecione **Solicitar dados** - **Solicitar informações do SysInspector**. Os logs podem ser obtidos somente de produtos da geração 4.x e posteriores; versões anteriores não são compatíveis com esse recurso. Uma janela com as seguintes opções será exibida:

- **Criar instantâneo (registrar também o log resultante no cliente)** - salva uma cópia do log no computador cliente.
- **Incluir comparação com o último snapshot antes de uma hora especificada** - exibe um log comparativo; logs comparativos são criados pela fusão do log atual com um log anterior, se disponível. O ERA escolherá o primeiro log

que for anterior à data especificada.

Clique em **OK** para obter os logs selecionados e salve-os no servidor. Para abrir e visualizar os logs, proceda da seguinte forma:

As opções do ESET SysInspector para estações de trabalho clientes individuais podem ser encontrados na guia **Propriedades do cliente** - **SysInspector**. A janela será dividida em três seções; a seção principal mostra informações de texto sobre os logs mais recentes do cliente especificado. Clique em **Atualizar** para carregar a configuração mais atual.

A seção intermediária da janela **Opções de solicitação** é praticamente idêntica à janela, que aparece no processo descrito acima de solicitação de logs de estações de trabalho clientes. O botão **Solicitar** será usado para obter um log do ESET SysInspector do cliente.

A seção inferior consiste nestes botões:

- **Visualizar** - abre o log relacionado na seção superior diretamente no ESET SysInspector.
- **Salvar como...** - salva o log atual em um arquivo. **Em seguida, execute o Visualizador do ESET SysInspector para visualizar este arquivo** abre automaticamente o log depois que ele for salvo (como seria depois de clicar em **Visualizar**).

As ações de gerar e exibir novos arquivos de log às vezes podem ficar lentas pelo cliente local, devido ao tamanho do log e velocidade de transferência de dados. A data e a hora atribuídas a um log no **Propriedades do cliente** > **SysInspector** marcam a data e hora de entrega para o servidor.

5.6 Assistente de fusão de regras de firewall

O Assistente de fusão de regras de firewall permite que você mescle regras de firewall para clientes selecionados. Isso é especialmente útil quando você precisa criar uma única configuração contendo todas as regras de firewall que foram coletadas pelos clientes no modo de aprendizado. A configuração resultante pode ser então enviada para clientes através de uma tarefa de configuração ou pode ser aplicada como uma política.

O assistente está acessível do menu suspenso **Ferramentas** e do menu de texto na guia **Clientes** depois de clicar com o botão direito do mouse nos clientes selecionados (os clientes selecionados serão então automaticamente adicionados aos itens selecionados na primeira etapa).

OBSERVAÇÃO: Para realizar esta ação com êxito, todos os clientes selecionados deverão ter a configuração mais recente armazenada (enviada ou replicada) no servidor. Você precisa escolher os clientes ou grupos de clientes dos quais as regras de firewall serão mescladas. Na próxima etapa, você verá uma lista de clientes selecionados e seu status de configuração. Se a configuração de um cliente não estiver no servidor, você poderá solicitá-la clicando no botão **Solicitar**. Por fim, você poderá escolher quais das regras mescladas serão usadas na configuração e salvá-las em um arquivo *.xml*.

6. Opções do ERA Server

O ERA Server pode ser facilmente configurado diretamente do ERA Console conectado ao ERA Server - a opção **Ferramentas** > **Opções do servidor...**.

6.1 Geral

A guia **Geral** mostra as informações básicas do ERA Server:

- **Informações do servidor** - nesta seção, você pode ver as informações básicas do ERA Server. Clique no botão Alterar senha... para abrir a guia Segurança 93 das Opções do ERA Server.
- **Informações de licença** - mostra o número de licenças clientes de produtos de segurança da ESET que você adquiriu e a versão atual do sistema antivírus NOD32 ou ESET Smart Security no computador do servidor. Se sua licença tiver expirado e você tiver adquirido uma nova, clique no botão Gerenciador de licenças 92 para abrir uma caixa de diálogo onde você poderá procurar uma nova licença para ativar o ERA.
- **Versão do banco de dados de assinaturas de vírus** - mostra a versão atual da versão do banco de dados de assinaturas de vírus (com base nas informações de atualização fornecidas e os produtos de segurança usados).
- **Desempenho** - mostra as informações de desempenho geral e conexão servidor-cliente.

6.1.1 Gerenciamento de licenças

Para que o ERA funcione devidamente, uma chave de licença deverá ser carregada. Depois da compra, as chaves de licença serão enviadas junto com seu nome de usuário e senha para seu e-mail. O **Gerenciador de licenças** serve para gerenciar licenças.

No ERA 3.x e versões posteriores, foi adicionado suporte para várias chaves de licença. Esse recurso torna o gerenciamento de chaves de licença mais conveniente.

A principal janela do Gerenciador de licenças está acessível em **Ferramentas** > **Gerenciador de licenças**.

Para adicionar uma nova chave de licença:

1) Acesse **Ferramentas** > **Gerenciador de licenças** ou pressione **CTRL + L** em seu teclado.

2) Clique em **Procurar** e localize o arquivo da chave de licença desejado (as chaves de licença têm a extensão *.lic*).

3) Clique em **Abrir** para confirmar.

4) Verifique se as informações de chave de licença estão corretas e selecione **Carregar para servidor**.

5) Clique em **OK** para confirmar.

O botão **Carregar para servidor** estará ativo somente se você tiver selecionado uma chave de licença (usando o botão **Procurar**). Informações sobre a chave de licença visualizada atualmente são mostradas nessa parte da janela. Isso permite uma verificação final antes de a chave ser copiada para o servidor.

A parte central da janela exibe informações sobre a chave de licença que é atualmente usada pelo servidor. Para ver detalhes sobre todas as chaves de licença presentes no servidor, clique no botão **Detalhes...**.

O ERAS tem a capacidade de selecionar a chave de licença mais relevante e mesclar várias chaves em uma. Se mais de uma chave de licença for carregada, o ERAS sempre tentará encontrar a chave com a maioria dos clientes e com a data de expiração mais no futuro.

A capacidade de mesclar várias chaves funcionará se todas as chaves forem de propriedade do mesmo cliente. Mesclar licenças é um processo simples que cria uma nova chave contendo todos os clientes envolvidos. A data de expiração da nova chave de licença se torna a data de expiração que expiraria primeiro.

A parte inferior da janela do Gerenciador de licenças é dedicada a notificações quando há um problema com licenças. As opções disponíveis incluem:

- **Avisar se o servidor estiver prestes a expirar em 20 dias** - exibe um aviso X dias antes de a licença expirar
- **Avisar somente se isso fizer com que o número de clientes na licença fique abaixo do número de clientes reais no banco de dados do servidor** - ative essa opção para mostrar um aviso somente se a expiração da chave de licença ou uma parte da licença for causar uma diminuição no número de clientes abaixo do número de clientes atualmente

conectados ou clientes no banco de dados do ERAS.

- **Avisar se houver somente 10% clientes livres restantes na licença do servidor** - o servidor exibirá um aviso se o número de clientes livres ficar abaixo do valor especificado (em %)

O ERAS tem capacidade para mesclar várias licenças de vários clientes. Esse recurso deve ser ativado por uma tecla especial. Se você precisar de uma chave especial, especifique-a em seu pedido ou entre em contato com seu distribuidor da ESET local.

6.2 Segurança

As versões 3.x e posteriores de soluções de segurança da ESET (ESET Smart Security, etc.) oferecem proteção de senha para comunicação descriptografada entre o cliente e o ERAS (comunicação no protocolo TCP, porta 2222). Versões anteriores (2.x) não têm essa funcionalidade. Para fornecer compatibilidade retrógrada para versões anteriores, o modo **Habilitar acesso não autenticado para clientes** deverá ser selecionado. A guia **Segurança** contém opções que permitem que o administrador use simultaneamente soluções de segurança 2.x e 3.x na mesma rede.

Proteção para comunicação com um ERA Server.

OBSERVAÇÃO: se a autenticação estiver habilitada no ERAS e em todos os clientes (geração 3.x e posteriores), a opção **Habilitar acesso não autenticado para clientes** poderá ser desabilitada.

Configurações de segurança do console

- **Usar autenticação do Windows/domínio -** habilita a autenticação do Windows/domínio e permite que você defina grupos de administrador (com acesso completo ao ERA Server), bem como a grupos com acesso somente leitura (opção **Tratar todos os outros usuários com acesso somente leitura**). Se esta caixa de seleção for marcada, a opção **Permitir acesso somente leitura para usuários Windows/Domínio sem um usuário de servidor ERA determinado** torna-se ativa e pode ser selecionada. Essa opção garante que esses usuários não possam alterar as configurações no ERAC. Se você quiser atribuir usuários ERA Server, clique em **Gerenciador de usuários**.
- O acesso ao console do usuário pode ser gerenciado através da ferramenta Gerenciador de usuários 94.

Configurações de segurança do servidor

- **Senha para clientes** - define a senha para clientes acessando o ERAS.
- **Senha para replicação** - define a senha para ERA Servers inferiores se replicado para o ERAS especificado.
- **Senha para Instalador remoto da ESET (agente)** - define a senha para o agente do instalador para acesso ao ERAS (relevante para instalações remotas).
- **Habilitar acesso não autenticado para clientes (produtos de segurança da ESET)** - permite o acesso ao ERAS aos clientes que não têm uma senha válida especificada (se a senha atual for diferente de **Senha para clientes**).
- **Habilitar acesso não autenticado para replicação** - permite o acesso ao ERAS para clientes de ERA Servers inferiores que não tiverem uma senha válida para replicação especificada.
- **Habilitar acesso não autenticado para instalador remoto da ESET (agente)** - habilita o acesso para o ERAS para o instalador remoto da ESET que não tiver uma senha válida especificada.

OBSERVAÇÃO: **Padrão** só restaura as configurações predefinidas - ele não reinicia suas senhas.

OBSERVAÇÃO: se você quiser aumentar a segurança, poderá usar senhas complexas. Acesse **Ferramentas** > **Editor de configuração da ESET** > **Administração remota** > **ERA Server** > **Configurações** > **Segurança** > **Requer senha complexa** e defina essa opção como **Sim**. Quando essa opção estiver habilitada, cada nova senha precisará ter pelo menos 8 caracteres e deverá ter letras minúsculas, maiúsculas e um caractere que não seja letra.

6.2.1 Gerenciador de usuários

A ferramenta **Gerenciador de usuários** permite que você administre as contas de usuários para autenticação no console-servidor. As contas de administrador (acesso total) e somente leitura são predefinidas.

Clique em **Novo** para adicionar uma nova conta de usuário para a autenticação no console-servidor. Defina o **Nome de usuário**, a **Senha** e as **Permissões** específicas.

O campo **Descrição** destina-se para descrições personalizadas do usuário, e não é obrigatório.

As **Permissões** definem o nível de acesso que o usuário tem e as tarefas específicas que ele pode realizar. Você pode alterar a senha de acesso ao console 94 para cada usuário acessando o console ao selecionar o usuário específico e, em seguida, clicar em **Alterar...** ao lado de **Senha para autenticação no console**.

OBSERVAÇÃO: as permissões das contas predefinidas (administrador e somente leitura) não podem ser modificadas.

Você pode vincular um ou mais **Grupos de autenticação de domínio/Windows** a um servidor ERA Server selecionado. Se um grupo do Windows/domínio for atribuído a vários usuários, o primeiro usuário da lista de usuários será usado. As etapas para cima e para baixo ao lado da lista de usuário definem a ordem de usuários.

6.2.2 Senha de acesso ao console

Para alterar a senha de acesso ao Console, clique em **Arquivo** > **Alterar senha** ou altere a senha usando o Gerenciador de usuários 94. Insira sua senha antiga e, em seguida, a nova senha duas vezes (para confirmação). Se você marcar a caixa de seleção ao lado de **Também alterar senha armazenada em cache**, a senha armazenada em cache usada no início do aplicativo (para que o usuário não precise digitá-la sempre que acessar o ERAC) será alterada.

OBSERVAÇÃO: as senhas que você definir nessa caixa de diálogo são enviadas diretamente para o servidor. Isso significa que a alteração será realizada imediatamente depois de clicar em **OK** e não poderá ser revertida.

6.3 Manutenção do servidor

Se corretamente configurado na guia **Manutenção do servidor**, a manutenção do banco de dados ERA Server será realizada automaticamente e ele será otimizado, sem a necessidade de configuração adicional. Você pode definir as seguintes configurações de limpeza:

- **Parâmetros de coleta de log...** - define o nível de logs que são recebidos pelo servidor.
- **Configurações de limpeza...** - exclui os logs pelo parâmetro de tempo.
- **Configurações avançadas de limpeza...** - exclui os logs pela contagem de registros de log.

Especifique quantas entradas de log devem ser mantidas depois da limpeza, bem como o nível de logs que são recebidos pelo servidor. Por exemplo, se você escolher **Excluir todos os logs de ameaça, exceto os últimos 600.000** em Configurações avançadas de limpeza por contagem de registros de log 96 e o nível de Parâmetros de coleta de log 95 para **Ameaças** for definido como **Nível 3 - Acima+Normal**, os últimos 600.000 registros contendo informações sobre erros críticos, notificações de alerta e notificações informativas serão mantidos no Banco de dados. Você também pode limitar as entradas de log usando o Limpeza por parâmetro de tempo 95.

Agenda de limpeza - realiza as opções selecionadas acima no intervalo especificado. Clique em **Alterar...** ao lado dessa opção para definir os parâmetros de tempo. Clique em **Limpar agora** para iniciar a limpeza imediatamente.

Compactar e reparar agenda - compacta o banco de dados no intervalo de tempo especificado na hora especificada. Compactar e reparar elimina inconsistências e falhas, e torna a comunicação com o banco de dados mais rápida. Clique em **Alterar...** ao lado dessa opção para definir os parâmetros de tempo. Clique em **Compactar agora** para começar a compactar e reparar imediatamente.

OBSERVAÇÃO: as ferramentas **Limpeza** e **Compactar e reparar** são demoradas e exigem recursos; portanto, recomendamos agendar sua execução quando houver um mínimo de carga no servidor (por exemplo, execute a Limpeza à noite, e a Compactar e reparar aos fins de semana).

Por padrão, entradas e logs anteriores a três/seis meses serão excluídos e a tarefa **Compactar e reparar** será realizada a cada quinze dias.

6.3.1 Parâmetros de coleta de log

Defina o nível de logs que são enviados para o servidor. Selecione o nível de detalhamento para cada tipo de log usando os menus suspensos correspondentes.

Nenhum - Nenhum log será enviado para o servidor. Como o cliente não registra nada em log usando essa configuração, o ERA não poderá receber quaisquer logs.

Nível 1 - Avisos críticos - somente erros críticos. Erros críticos não são registrados nas guias **Controle de Web** ou **Controle de dispositivo**, pois o cliente não pode produzir esses logs.

Nível 2 - Acima + Avisos - o mesmo que nível 1, mais notificações de alerta.

Nível 3 - Acima + Normal - o mesmo que nível 2, mais notificações informativas. Esse nível de detalhamento é intitulado **Informações** em vez de **Normal** por parte do cliente.

Nível 4 - Acima + diagnóstico - o mesmo que nível 3, mais notificações diagnósticas. Esse nível de detalhamento precisa ser definido por parte do cliente também, a configuração padrão no cliente é o nível de registro em log **Informações**.

Todos - todos os logs serão recebidos.

6.3.2 Limpeza por parâmetro de tempo

Principais de limpeza para limpeza pelo intervalo de tempo:

- **Excluir clientes não conectados nos últimos X meses (dias)** - exclui todos os clientes que não se conectaram ao ERAS por mais tempo do que o número especificado de meses (ou dias).
- **Excluir logs de ameaça anteriores a X meses (dias)** - exclui todos os incidentes de vírus (ameaças detectadas) anteriores ao número especificado de meses (ou dias).
- **Excluir logs de firewall anteriores a X meses (dias)** - exclui todos os logs de firewall anteriores ao número especificado de meses (ou dias).
- **Excluir logs de evento anteriores a X meses (dias)** - exclui todos os eventos de sistema anteriores ao número especificado de meses (ou dias).
- **Excluir logs do HIPS anteriores a X meses (dias)** - todos os logs do HIPS (Host Intrusion Prevention System, Sistema de prevenção de intrusos de host) anteriores ao número especificado de meses (ou dias).
- **Excluir logs de controle de dispositivo anteriores a X meses (dias)** - exclui todos os logs de controle de dispositivo anteriores ao número especificado de meses (ou dias).
- **Excluir logs de controle da Web anteriores a X meses (dias)** - exclui todos os logs de controle da Web anteriores ao número especificado de meses (ou dias).
- **Excluir logs de antispam anteriores a X meses (dias)** - exclui todos os logs de antispam anteriores ao número especificado de meses (ou dias).
- **Excluir logs de lista cinza anteriores a X meses (dias)** - exclui todos os logs de lista cinza anteriores ao número especificado de meses (ou dias).
- **Excluir logs de rastreamento anteriores a X meses (dias)** - exclui todos os logs de scanner anteriores ao número especificado de meses (ou dias).
- **Excluir logs móveis anteriores a X meses (dias)** - exclui todos os logs móveis anteriores ao número especificado de meses (ou dias).
- **Excluir entradas de quarentena sem clientes que sejam anteriores a X meses (dias)** - exclui todas as entradas de quarentena que não forem atribuídas a qualquer cliente e que sejam anteriores ao número especificado de meses (ou dias).
- **Excluir entradas de computadores não registrados anteriores a X meses (dias)** - exclui todas as entradas de computadores não registrados (computadores que não são gerenciados pelo ERA) anteriores ao número especificado de meses (ou dias).
- **Exclui entradas de tarefas somente com estado concluído que sejam anteriores a X meses (dias)** - exclui todas as entradas de tarefas para tarefas concluídas e realizadas anteriores ao número especificado de meses (ou dias).

- **Exclui todas as entradas de tarefas que sejam anteriores a X meses (dias)** - exclui todas as entradas de tarefas (em qualquer estado) anteriores ao número especificado de meses (ou dias).

6.3.3 Configurações avançadas de limpeza por contagem de registros de log

Configurações avançadas de limpeza para avançada por contagem de registros de log:

- **Excluir logs de ameaça, exceto últimos X registros** - exclui todos os incidentes de vírus (ameaças detectadas), exceto o número especificado de registros.
- **Excluir logs de firewall, exceto últimos X registros** - exclui todos os logs de firewall, exceto o número especificado de registros.
- **Excluir logs de evento, exceto últimos X registros** - exclui todos os eventos do sistema, exceto o número especificado de registros.
- **Excluir logs do HIPS, exceto últimos X registros** - exclui todos os logs do HIPS (Host Intrusion Prevention System, Sistema de prevenção de intrusos de host), exceto o número especificado de registros.
- **Excluir todos os logs de controle do dispositivo, exceto o último** - exclui todos os logs de controle do dispositivo, exceto o número especificado de registros.
- **Excluir todos os logs de controle da web, exceto o último** - exclui todos os logs de controle da web, exceto o número especificado de registros.
- **Excluir logs de antispam, exceto últimos X registros** - exclui todos os logs de antispam, exceto o número especificado de registros.
- **Excluir logs de lista cinza, exceto últimos X registros** - exclui todos os logs de lista cinza, exceto o número especificado de registros.
- **Excluir logs de rastreamento, exceto últimos X registros** - exclui todos os logs de rastreamento, exceto o número especificado de registros.
- **Excluir logs de celular, exceto últimos X registros** - exclui todos os logs de celular, exceto o número especificado de registros.

6.4 Registro em log

Para definir parâmetros para manutenção do banco de dados, selecione **Ferramentas/Opções do servidor** no menu principal do ERA Console.
A manutenção do banco de dados fornece opções para manter regularmente os logs transparentes e permite a compactação do banco de dados principal do ERA, a fim de preservar espaço.

1. Log de auditoria

O log de auditoria monitora e registra em log todas as alterações na configuração e ações realizadas por todos os usuários do ERAC.

- Se a opção **Registrar em arquivo de texto** for selecionada, novos arquivos de log serão criados (**Girar quando superior a X MB**) e excluídos diariamente (**Excluir logs girados anteriores a X dias**). Você também pode alterar o detalhamento do log no menu suspenso à esquerda.

Clique em Exibir log 98 para exibir o log de auditoria atual.

- A opção **Registrar em log de aplicativo de SO** permite que informações sejam copiadas no log do visualizador de eventos do sistema (**Painel de controle do Windows** > **Ferramentas administrativas** > **Visualizador de eventos**). Você também pode alterar o detalhamento do log no menu suspenso à esquerda.
- A opção **Registrar no Syslog** envia uma mensagem do syslog para o servidor syslog especificado em uma porta especificada (o servidor padrão é o host local, a porta padrão é 514). Para configurações avançadas do syslog, acesse **Ferramentas** > **Opções do servidor** > **Avançadas** >**Editar configurações avançadas...** > **Configuração** > **Registro em log**. Você pode editar aqui as opções do syslog - nome do servidor syslog, porta do servidor syslog, recurso do syslog e o detalhamento de syslog.

OBSERVAÇÃO: a gravidade do Syslog deverá ser configurada para cada tipo de log. Para o log de servidor, é a configuração **Recurso do Syslog para log de servidor**, para o log de depuração é a configuração **Log de recurso do syslog para depuração**. Para esses logs, a gravidade do syslog é a seguinte:

Detalhamento do ERA	Gravidade do Syslog
Nível 1 (Informações)	LOG_INFO //6
Nível 2 (Erro)	LOG_INFO //3
Nível 3 (Aviso)	LOG_INFO //4
Nível 4,5 (Depuração)	LOG_INFO //7

O **Detalhamento** de um log significa o nível de detalhes em um log e as informações incluídas.

- **Nível 1 - Usuários e grupos** - registro em log da atividade relacionada ao grupo e ao usuário (grupos estáticos, grupos paramétricos, adicionar/remover cliente de um grupo, etc.).
- **Nível 2 - Acima + Ações de cliente** - Acima + toda a atividade relacionada ao cliente ERA (definir/limpar sinalizador Novo, definir política de cliente, solicitar dados, etc.).
- **Nível 3 - Acima + Tarefas e notificações** - Acima + toda a atividade relacionada a tarefas (criar/excluir tarefa, criar/excluir notificação, etc.).
- **Nível 4 - Acima + Relatórios** - Acima + toda a atividade relacionada a relatórios (criar/excluir relatório, selecionar excluir modelo de relatório, etc.).
- **Nível 5 - Todos os eventos** - toda a atividade relacionada a log (limpar log do HIPS, limpar log de ameaça, etc.).

2. Log de servidor

Durante a execução, o ERA Server cria um log de servidor (**Nome de arquivo do log**) sobre sua atividade que é configurável (**Detalhamento de log**).

OBSERVAÇÃO: Por padrão, a saída do arquivo de texto é salva no arquivo *%ALLUSERSPROFILE%\Application Data\Eset\ESET Remote Administrator\Server\logs\era.log*

- Se a opção **Registrar em arquivo de texto** for selecionada, novos arquivos de log serão criados (**Girar quando superior a X MB**) e excluídos diariamente (**Excluir logs girados anteriores a X dias**).

OBSERVAÇÃO: Na seção **Registrar em arquivo de texto**, recomendamos deixar o **Detalhamento de log** no *Nível 2 - Acima + Erros de sessão* e aumentá-lo somente se você tiver um problema ou for avisado para fazê-lo pelo Atendimento ao cliente da ESET.

- A opção **Registrar em log de aplicativo de SO** permite que informações sejam copiadas no log do visualizador de eventos do sistema (**Painel de controle do Windows** > **Ferramentas administrativas** > **Visualizador de eventos**).

- A opção **Registrar no Syslog** envia uma mensagem do syslog para o servidor syslog especificado em uma porta especificada (o servidor padrão é o host local, a porta padrão é 514). Para configurações avançadas do syslog, acesse **Ferramentas** > **Opções do servidor** > **Avançadas** >**Editar configurações avançadas...** > **Configuração** > **Registro em log.** Você pode editar aqui as opções do syslog - nome do servidor syslog, porta do servidor syslog, instalação syslog e o detalhamento de syslog.

O **Detalhamento** de um log significa o nível de detalhes em um log e as informações incluídas.

- **Nível 1 - Informações críticas** - comportamento de falha (nesse caso, entre em contato com o Atendimento ao cliente da ESET).
- **Nível 2 - Acima + Informações importantes sobre sessão** - informações sobre comunicação com o servidor (quem se conectou ao ERA Server, quando e por que).
- **Nível 3 - Acima + Várias informações** - informações sobre processos internos no ERA Server.
- **Nível 4 - Acima + Instalador** - informações sobre o agente einstaller.exe (informações sobre o ERA Server - conexão/desconexão do agente e os resultados).
- **Nível 5 - Acima + Clientes** - informações sobre o cliente (informações sobre o ERA Server, conexão/desconexão do cliente e os resultados).

OBSERVAÇÃO: Recomendamos deixar o detalhamento de log definido como Nível 2 - Acima + Erros de sessão. Altere o nível de log somente se você estiver tendo problemas ou se for orientado a fazê-lo pelo Atendimento ao cliente da ESET.

3. A opção **Log de depuração** do banco de dados deve ser desabilitada em circunstâncias normais - ela é usada para resolução de problemas do banco de dados. Clique em **Ferramentas** > **Opções do servidor** > **Avançadas** > **Editar configurações avançadas...** > **Configuração** > **Registro em log** > **Compactação de log de depuração girado** para configurar o nível de compactação para logs girados individuais.

6.4.1 Visualizador do log de auditoria

O **Log de auditoria** monitora e registra em log todas as alterações na configuração e ações realizadas por usuários do ERAC. Isso ajuda o administrador a controlar toda a atividade relacionada ao ERAC, incluindo possível acesso não autorizado.

OBSERVAÇÃO: o Visualizador do log de auditoria exibe alterações registradas no banco de dados. O Log de auditoria não inclui outros logs (como log de arquivo e outros).

No lado esquerdo, você pode ver o **Filtro** usado para filtrar entradas do **Log de auditoria**. Você também pode selecionar o número de **Itens a serem exibidos** no menu suspenso neste módulo, no lado direito superior abaixo da lista de entradas do **Log de auditoria**.

Filtro:

- **De/a** - selecione o horário específico inicial (de)/a (final) durante o qual os logs serão filtrados. Selecionar ambas as opções e selecionar horários cria um intervalo de tempo.
- **Usuário** - insira os usuários para os quais deseja que os logs sejam exibidos.
- **Nome de login de domínio** - insira o nome de login de domínio do usuário para o qual deseja que os logs sejam exibidos.
- **Endereço IP** - selecione a opção desejada (**Endereço**, **Intervalo** ou **Máscara**) e insira os endereços nos campos apropriados. Essas opções são comuns para os endereços IPv4 e IPv6.
- **Tipos de ação** - selecione as ações que você deseja que sejam exibidas nos logs de auditoria. Por padrão, todas elas são selecionadas e, portanto, exibidas.
- **Aplicar filtro** - clicar nesse botão aplicará imediatamente os parâmetros de filtro ao **Log de auditoria**.
- **Padrão** - clicar nesse botão redefinirá os parâmetros de filtro para seu estado padrão.

Lista de entradas do log de auditoria:

- **Data** - data na qual a ação foi realizada. Essa data e hora são baseadas nas configurações de horário da máquina do servidor.
- **Usuário** - usuário do ERAC que realizou a ação.
- **Nome de login** - nome de login do domínio do Windows do usuário que realizou a ação. Isso será exibido somente quando o tipo de login do Windows/domínio for usado.
- **Endereço IP do console** - endereço IP do console do qual a ação foi realizada pelo usuário do ERAC.
- **Ação** - ação que foi realizada pelo usuário.
- **Objeto** - número de objetos afetados por essa ação.

OBSERVAÇÃO: informações adicionais (se disponíveis) serão mostradas depois de um duplo clique em uma linha específica no log.

6.5 Replicação

Para definir as configurações do ERA Server, clique em **Ferramentas** > **Opções do servidor** da janela principal do programa do ERA Console.

A replicação é usada em grandes redes onde vários ERA Servers estão instalados (p. ex., uma empresa com várias filiais). A guia **Configurações de replicação** permite que você configure a replicação de dados entre vários ERA Servers em execução em sua rede. Para saber como configurar vários ERA Servers em sua organização, consulte o capítulo Configurando servidores de RA em redes grandes 99.

Para configurar a replicação, use as seguintes opções de replicação:

Configurações de replicar "para"

- **Habilitar replicação "para"** - habilita a replicação em uma rede grande, como descrito no capítulo Replicação 99.
- **Servidor superior** - endereço IP ou nome do ERA Server superior, que coletará dados do ERA Server local.

- **Porta** - especifica a porta usada para replicação.
- **Replicar a cada XX minutos** - configura o intervalo de replicação.
- **Replicar: Log de ameaça**, **Log de firewall**, **Log de eventos**, **Log de rastreamento**, **Log de mobile**, **Log de quarentena** - se essas opções forem selecionadas, todas as informações exibidas nas guias Clientes, Log de ameaça, Log de firewall, Log de eventos, Log de rastreamento, Tarefas, Log de mobile e Log de quarentena serão replicadas em linhas e colunas individuais. As informações não armazenadas diretamente no banco de dados, mas em arquivos individuais (ou seja, formato *.txt* ou *.xml*) não poderão ser replicadas. Habilite essas opções para também replicar entradas nesses arquivos.
- **Replicar automaticamente: Detalhes do cliente**, **Detalhes de log de ameaça**, **Detalhes de log de rastreamento**, **Detalhes de log de mobile**, **Arquivos em quarentena** - essas opções habilitam a replicação automática das informações complementares armazenadas em arquivos individuais (elas também podem ser obtidas por download sob demanda clicando em **Solicitar**).
- **Tipo de log** - define o tipo de eventos a serem replicados (alerta, evento, rastreamento) para o ERA Server superior.
- **Replicar automaticamente...** - habilita a replicação periódica. Quando não habilitada, a replicação poderá ser acionada manualmente.

Status de replicação "para"

- **Replicar até agora** - inicia o processo de replicação.
- **Marcar todos os clientes para replicação** - se habilitada, todos os clientes serão replicados, incluindo aqueles sem alterações.

Configurações de replicar "de"

- **Habilitar replicação "de"** - habilita o ERA Server local para coletar dados de outros servidores relacionados no campo **Servidores permitidos**. Use vírgulas para separar vários ERA Servers.
- **Permitir replicação de qualquer servidor** - se esta opção for marcada, é possível replicar a partir de qualquer servidor. Marcar esta caixa de seleção desabilita o campo **Servidores permitidos**.

6.5.1 Replicação em grandes redes

A replicação é usada em grandes redes onde vários ERA Servers estão instalados (p. ex., uma empresa com várias filiais). Para obter mais informações, consulte o capítulo Instalação 21.

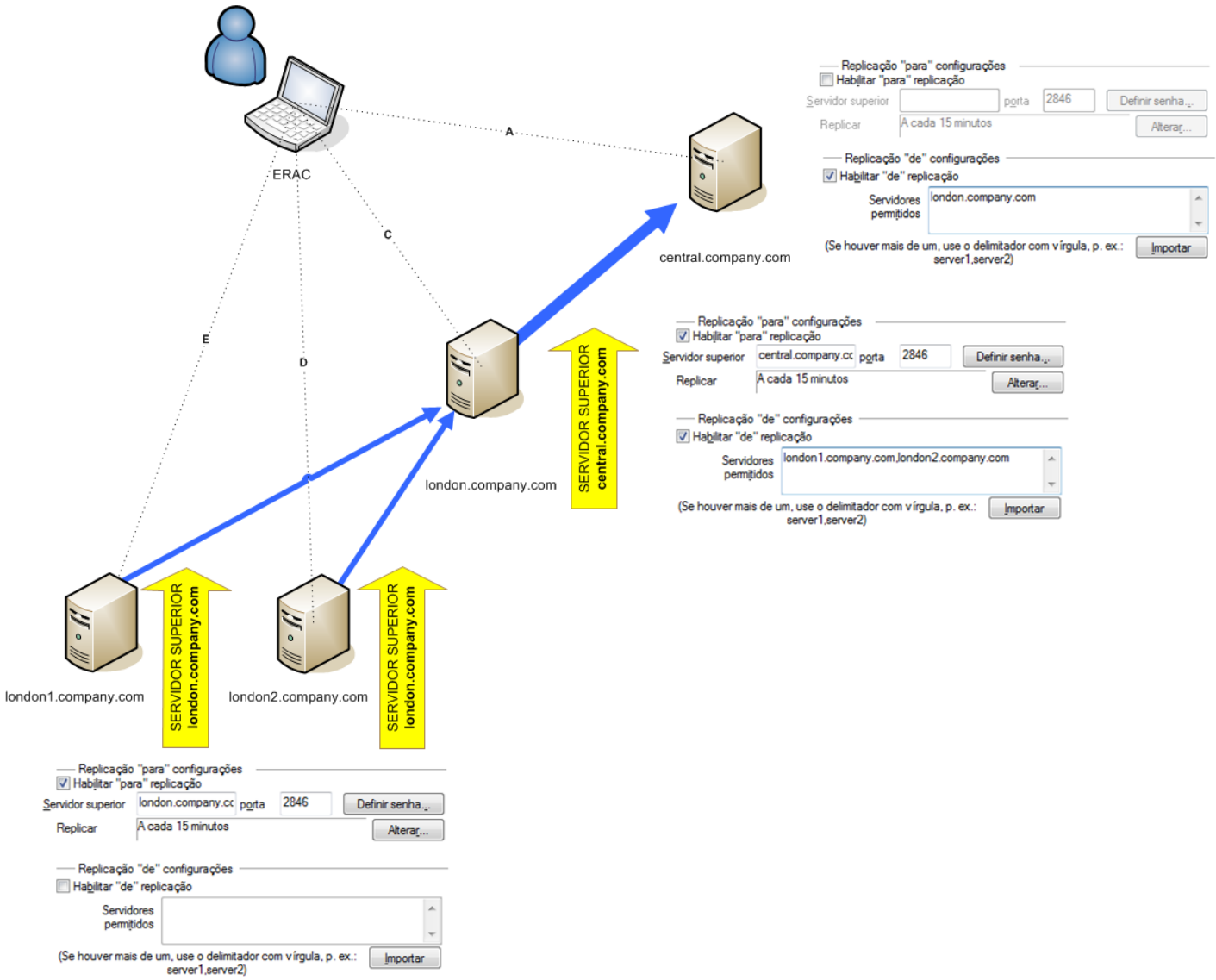
As opções na guia Replicação (**Ferramentas > Opções do servidor...**) são divididas em duas seções:

- Configurações de replicar "para"
- Configurações de replicar "de"

A seção **Configurações de replicar "para"** é usada para configurar ERA Servers inferiores. A opção **Habilitar replicação "para"** deverá estar habilitada e o endereço IP ou nome do ERAS principal (servidor superior) inserido. Os dados do servidor inferior serão então replicados para o servidor principal. As **Configurações de replicar "de"** permitem que os ERA Servers principais (superiores) aceitem dados de ERA Servers inferiores ou os transfira para seus servidores principais. A opção **Habilitar replicação "de"** deverá estar habilitada e os nomes de servidores inferiores deverão ser definidos (delimitados por vírgula).

Ambas essas opções deverão estar habilitadas para os ERA Servers localizados em qualquer parte no centro da hierarquia de replicação (ou seja, têm servidores superiores e inferiores).

Todos os cenários previamente mencionados estão visíveis na figura a seguir. Os computadores bege representam ERA Servers individuais. Cada ERAS é representado por seu nome (que deve ser o mesmo que *%Computer Name%* para evitar confusão) e as configurações correspondentes na janela da caixa de diálogo.



Outras opções que influenciam o comportamento de replicação de servidores incluem:

- **Replicar log de ameaça**, **Replicar log de firewall**, **Replicar log de evento**, **Replicar log de rastreamento**, **Replicar log de mobile**, **Replicar log de quarentena**
  Se essas opções forem selecionadas, todas as informações exibidas na guia **Clientes**, **Log de ameaça**, **Log de firewall**, **Log de evento**, **Log de rastreamento**, **Log de mobile**, **Log de quarentena** e **Tarefas** serão replicadas em linhas e colunas individuais. As informações não armazenadas diretamente no banco de dados, mas em arquivos individuais (ou seja, formato *.txt* ou *.xml*) não poderão ser replicadas. Habilite essas opções para também replicar entradas nesses arquivos.

- **Replicar automaticamente detalhes de log de ameaça**, **Replicar automaticamente detalhes de log de rastreamento**, **Replicar automaticamente detalhes do cliente**, **Replicar automaticamente detalhes de log de mobile**, **Replicar automaticamente arquivos em quarentena**
  Estas opções permitem a replicação automática das informações complementares armazenadas em arquivos individuais. Elas podem ser obtidas por download sob demanda clicando-se no botão **Solicitar**.

OBSERVAÇÃO: alguns logs são replicados automaticamente, enquanto logs detalhados e logs de configuração de cliente são replicados somente sob demanda. Isso ocorre por que alguns logs contêm grandes quantidades de dados que podem não ser relevantes. Por exemplo, um log de rastreamento com a opção Registrar em log todos os arquivos habilitada consumirá uma quantidade significativa de espaço em disco. Tais informações geralmente não são necessárias e podem ser solicitadas manualmente. Os servidores filhos não enviam automaticamente informações sobre clientes excluídos. Portanto, os servidores superiores podem continuar armazenando informações sobre clientes excluídos de servidores inferiores. Se você quiser excluir um cliente da guia Cliente em servidores superiores, selecione a opção Permitir exclusão de clientes replicados no servidor subjacente localizada em **Opções do servidor** > **Avançadas** > **Editar configurações avançadas** > **Configuração** > **Replicação**.

Para definir o nível de manutenção de log no ERAS, clique em **Ferramentas** > **Opções do servidor** > **Avançadas** > **Editar configurações avançadas...** > **Configuração** > **Manutenção do servidor**.

Se você quiser replicar somente clientes com uma alteração de status, selecione a opção **Ferramentas** > **Opções do servidor** > **Replicação** > **Marcar todos os clientes para replicação por "Replicar até agora"**.

6.6 Atualizações

A janela **Atualizações**, localizada no módulo **Opções do servidor**, serve para definir parâmetros de atualização para o ESET Remote Administrator Server. A janela é dividida em duas seções: a superior relaciona opções de atualizações do servidor; a inferior é dedicada a parâmetros de imagem de atualização. Desde a versão 2.0, o ESET Remote Administrator Server inclui o recurso Servidor de imagem[102], que cria um servidor de atualização local para estações de trabalho clientes.

As descrições de todos os elementos e recursos são incluídas a seguir:

- **Servidor de atualização** - este é o servidor de atualização da ESET. Recomenda-se o uso do valor predefinido (seleção automática).
- **Intervalo de atualização** - especifica o intervalo máximo entre duas verificações consequentes para a disponibilidade novos arquivos de atualização.
- **Nome do usuário de atualização** - nome do usuário utilizado pelo ESET Remote Administrator para autenticação nos servidores de atualização.
- **Senha de atualização** - senha pertencendo ao nome de usuário fornecido.

As atualizações regulares do componente do programa e banco de dados de assinatura de vírus são importantes elementos para garantir a detecção de ameaças em tempo hábil. No entanto, os administradores de rede gerenciando grandes redes podem ocasionalmente ter problemas relacionados à atualização, como falsos alarmes ou problemas relacionados a módulos. Há três opções para se conectar a um servidor de atualização:

- **Atualização regular** - o banco de dados de assinatura de vírus é atualizado de servidores de atualização regular no momento em que forem publicados.
- **Modo de teste** - se a opção estiver habilitada, durante a atualização será feito o download de módulos beta. Isso não é recomendado em um ambiente de produção, somente para fins de testes.
- **Atualização adiada** - habilite essa opção para receber atualizações com um atraso de 12 horas, ou seja, atualizações testadas em um ambiente de produção e consideradas estáveis.

Para iniciar uma tarefa de atualização para fazer download de todos os componentes mais recentes do ESET Remote Administrator, clique em **Atualizar agora**. As atualizações podem conter funcionalidades ou componentes importantes; portanto, é vital se certificar de que as atualizações funcionem corretamente e automaticamente. Se tiver problemas com uma atualização, selecione **Limpar cache de atualização** para limpar a pasta com arquivos de atualização temporários. A opção **Imagem de PCU obtida por download** se tornará ativa quando for feito o download de uma atualização de PCU (*PCU - Program Component Upgrade, Atualização de componentes do programa*) e for necessário confirmar isso manualmente. Clique nesse botão para ver todas as atualizações de PCU disponíveis e o EULA. Para configurar a obtenção de imagem de PCU, acesse **Avançado** > **Editar configurações avançadas** e defina as configurações em **ESET Remote Administrator** > **ERA Server** > **Configuração** > **Imagem**.
A configuração de uma imagem no ESET Remote Administrator Server é a mesma que no ESET NOD32 Antivirus Business Edition e no ESET Smart Security Business Edition. As descrições de elementos importantes de imagem são incluídas a seguir:

- **Criar imagem de atualização** - ativa o recurso de imagem. Se essa opção estiver desabilitada, nenhuma cópia de atualização será criada.
- **Criar imagem dos componentes de programa selecionados** - permite que o usuário especifique variantes de idioma e tipos de componentes do programa que serão criados na imagem.
- **Preencher imagem com atualizações selecionadas do componente do programa somente sob demanda** - se habilitada, a imagem de PCUs não será feita automaticamente. Se você quiser habilitar a imagem de PCU, selecione a opção **Imagem de PCU obtida por download** em **Ferramentas** > **Opções do servidor** > **Atualizações**
- **Pasta Imagem** - diretório de rede ou local dedicado para armazenar arquivos de atualização.
- **Habilitar distribuição de atualização via HTTP** - permite que você acesse atualizações usando um servidor HTTP interno.
- **Porta de servidor HTTP** - define a porta na qual o ESET Remote Administrator Server fornecerá serviços de atualização.

- **Autenticação de servidor HTTP** - define o método de autenticação usado para acessar arquivos de atualização. As opções disponíveis são: **NENHUMA**, **Básica** e **NTLM**. Selecione **Básica** para utilizar a codificação base64, com autenticação básica. A opção **NTLM** fornece codificação usando um método de codificação seguro. Para autenticação, os usuários criados na estação de trabalho que compartilha os arquivos de atualização são utilizados.

Clique em **Padrão** na seção a seguir para restaurar valores predefinidos para todos os recursos nesta janela.

OBSERVAÇÃO: se o método de servidor HTTP estiver em uso, recomendamos um máximo de 400 clientes atualizando de uma imagem. Em redes maiores com mais clientes, recomendamos equilibrar atualizações de imagem entre mais servidores de imagem ERA (ou ESS/EAV). Se a imagem precisar ser centralizada em um único servidor, recomendamos usar outro tipo de servidor HTTP, como Apache. O ERA também é compatível com métodos adicionais de autenticação (p. ex., no Apache Web Server, é usado o método .htaccess).

O administrador deve inserir a chave de licença do produto para um produto adquirido, e inserir o nome de usuário e senha para ativar o recurso Imagem no ERAS. Se o administrador usar uma chave de licença, nome de usuário e senha para o ESET NOD32 Antivirus Business Edition, então posteriormente atualizar para o ESET Smart Security Business Edition, a chave de licença original, o nome de usuário e senha também deverão ser substituídos.

OBSERVAÇÃO: os clientes ESET NOD32 Antivirus também poderão ser atualizados usando uma licença do ESET Smart Security, mas não vice-versa.

6.6.1 Servidor de imagem

O recurso Imagem permite que um usuário crie um servidor de atualização local. Os computadores clientes não farão download de assinaturas de vírus de servidores da ESET na Internet, mas se conectarão a um servidor de Imagem local em sua rede. As principais vantagens dessa solução são economizar largura de banda de Internet e minimizar tráfego de rede, pois somente o servidor de imagem se conecta à Internet para atualizações em vez de centenas de máquinas clientes. Essa configuração significa que é importante para o servidor de Imagem estar sempre conectado à Internet.

Aviso: um servidor de Imagem que realizou uma atualização de componente do programa e não foi reiniciado pode causar uma interrupção. Nesse cenário, o servidor não seria capaz de fazer download de QUAISQUER atualizações ou distribui-las para estações de trabalho clientes. NÃO DEFINA ATUALIZAÇÕES AUTOMÁTICAS DE COMPONENTE DO PROGRAMA PARA PRODUTOS DO SERVIDOR DA ESET!

O recurso Imagem está disponível em dois locais:

- ESET Remote Administrator (Imagem em execução fisicamente no ERAS, gerenciável do ERAC)
- ESET Smart Security Business Edition ou ESET NOD32 Antivirus Business Edition (desde que a Business Edition tiver sido ativada por uma chave de licença).
- A Imagem também está disponível no ESET Endpoint Security e no ESET Endpoint Antivirus. Para obter mais informações, consulte a documentação do produto do cliente apropriado.

O administrador seleciona o método para ativar o recurso Imagem.

Em redes grandes, é possível criar vários servidores de Imagem (p. ex., para vários departamentos da empresa) e estabelecer um como central (em sedes da empresa) em estilo cascata - semelhante a uma configuração do ERAS com vários clientes.

O administrador deve inserir a chave de licença do produto para um produto adquirido, e inserir o nome de usuário e senha para ativar o recurso Imagem no ERAS. Se o administrador usar uma chave de licença, nome de usuário e senha para o ESET NOD32 Antivirus Business Edition, então posteriormente atualizar para o ESET Smart Security Business Edition, a chave de licença original, o nome de usuário e senha também deverão ser substituídos.

OBSERVAÇÃO: os clientes ESET NOD32 Antivirus também poderão ser atualizados usando uma licença do ESET Smart Security, mas não vice-versa. Isso também se aplica ao ESET Endpoint Antivirus e ESET Endpoint Security.

6.6.1.1 Operação do servidor de imagem

O computador hospedando o servidor de imagem sempre deve estar em execução e conectado à Internet ou a um servidor de imagem superior para replicação. Os pacotes de atualização do servidor de imagem podem ser baixados de duas formas:

1. Usando o protocolo HTTP (recomendado)

2. Usando uma unidade de rede compartilhada (SMB)

Os servidores de atualização da ESET usam o protocolo HTTP com autenticação. Um servidor de imagem central deve acessar os servidores de atualização com um nome de usuário (geralmente na seguinte forma: *EAV-XXXXXXX*) e senha.

O servidor de imagem que faz parte do ESET Smart Security/ESET NOD32 Antivirus tem um servidor HTTP integrado (variante 1).

OBSERVAÇÃO: se você decidir usar o servidor HTTP integrado (sem autenticação), certifique-se de que ele não estará acessível de fora de sua rede (ou seja, para clientes não incluídos em sua licença). O servidor não deve estar acessível da Internet.

Por padrão, o servidor HTTP integrado realiza a escuta na porta TCP 2221. Certifique-se de que essa porta não esteja sendo usada por qualquer outro aplicativo.

OBSERVAÇÃO: se o método de servidor HTTP estiver em uso, recomendamos um máximo de 400 clientes atualizando de uma imagem. Em redes maiores com mais clientes, recomendamos equilibrar atualizações de imagem entre mais servidores de imagem ERA (ou ESS/EAV). Se a imagem precisar ser centralizada em um único servidor, recomendamos usar outro tipo de servidor HTTP, como Apache. O ERA também é compatível com métodos adicionais de autenticação (p. ex., no Apache Web Server, é usado o método .htaccess).

O segundo método (pasta de rede compartilhada) requer o compartilhamento (direitos de "leitura" da pasta contendo pacotes de atualização. Nesse cenário, o nome de usuário e senha de um usuário com direitos de "leitura" para a pasta de atualização devem ser inseridos na estação de trabalho cliente.

OBSERVAÇÃO: as soluções clientes da ESET usam a conta de usuário SYSTEM e, portanto, têm diferentes direitos de acesso à rede de um usuário atualmente conectado. A autenticação é necessária mesmo se a unidade de rede estiver acessível para "Todos" e o usuário atual também puder acessá-las. Além disso, use os caminhos UNC para definir o caminho de rede para o servidor local. O uso do formato *DISK*:\ não é recomendado.

Se você decidir usar o método de pasta de rede compartilhada (variante 2), recomendamos que você crie um nome de usuário exclusivo (p. ex., NODUSER). Essa conta seria usada em todas as máquinas clientes para a finalidade exclusiva de baixar atualizações. A conta NODUSER deve ter direitos de "leitura" para a pasta de rede compartilhada, que contém os pacotes de atualização.

Para autenticação em uma unidade de rede, insira os dados de autenticação no formulário completo: *WORKGROUP\User* ou *DOMAIN\User*.

Além da autenticação, você também deve definir a origem de atualizações para soluções clientes da ESET. A origem de atualização é um endereço URL para um servidor local (*http://Mirror_server_name:port*) ou caminho UNC para uma unidade de rede: (*\\Mirror_server_name\share_name*).

6.6.1.2 Tipos de atualizações

Além das atualizações do banco de dados de assinaturas de vírus (que podem incluir atualizações de kernel de software da ESET), também estão disponíveis atualizações de componentes do programa. As atualizações de componentes do programa adicionam novos recursos aos produtos de segurança da ESET e exigem uma reinicialização.

O servidor de imagem permite que um administrador desative o download automático de atualizações do programa de servidores de atualização da ESET (ou de um servidor de imagem superior) e e desative sua distribuição a clientes. A distribuição pode ser posteriormente acionada manualmente pelo administrador, se ele estiver certo de que não haverá conflito entre a nova versão e os aplicativos existentes.

Esse recurso é especialmente útil se o administrador quiser baixar e usar atualizações do banco de dados de assinaturas de vírus quando também houver uma nova versão do programa disponível. Se uma versão de programa anterior for usada em conjunto com a versão do banco de dados de vírus mais recente, o programa continuará fornecendo a melhor proteção disponível. Além disso, recomendamos que você baixe e instale a versão mais recente do programa para obter acesso a novos recursos do programa.

Por padrão, os componentes do programa não serão automaticamente baixados e deverão ser configurados manualmente no ERAS. Para obter mais informações, consulte o capítulo Como ativar e configurar a Imagem 104.

6.6.1.3 Como ativar e configurar a Imagem

Se a Imagem estiver diretamente integrada ao ERA, conecte-se ao ERAS usando o ERAC e siga estas etapas:

- No ERAC, clique em **Ferramentas** > **Opções do servidor...** > **Atualizações**.
- No menu suspenso **Servidor de atualização**:, selecione **Escolher automaticamente** (as atualizações serão baixadas de servidores da ESET) ou insira o caminho *URL/UNC* em um servidor de Imagem.
- Defina o Intervalo de atualização para atualizações (recomendamos sessenta minutos).
- Se você tiver selecionado **Escolher automaticamente** na etapa anterior, insira o nome de usuário (Nome do usuário de atualização) e senha (Senha de atualização), que foram enviados após a compra. Se estiver acessando um servidor superior, insira um nome de usuário e senha de domínio válidos para esse servidor.
- Selecione a opção **Criar imagem de atualização** e insira um caminho para a pasta na qual armazenará os arquivos de atualização. Por padrão, há um caminho relativo para a pasta de Imagem. Desde que a caixa de seleção ao lado de **Fornecer arquivos de atualização através do servidor HTTP interno** esteja marcada, as atualizações estarão disponíveis na porta HTTP definida na **Porta do servidor HTTP** (por padrão, 2221). Defina **Autenticação** como **NENHUM** (para obter mais informações, consulte o capítulo Operação do servidor de imagem 103).

OBSERVAÇÃO: no caso de problemas com atualizações, selecione a opção **Limpar cache de atualização** para liberar a pasta na qual os arquivos de atualização temporários estão armazenados.

- A opção **Imagem de PCU obtida por download** permite que você ative a obtenção de imagem de componentes do programa. Para configurar a obtenção de imagem de PCU, acesse **Avançado > Editar configurações avançadas** e defina as configurações em **ESET Remote Administrator** > **ERA Server** > **Configuração > Imagem**.
- Selecione os componentes de idioma a serem baixados em **Avançado** > **Editar configurações avançadas...**, a ramificação **ERA Server** > **Configuração** > **Imagem** > **Criar imagem dos componentes de programa selecionados**. Componentes para todas as versões de idioma que serão usados na rede devem ser selecionados. Observe que o download de uma versão de idioma não instalada na rede aumentará desnecessariamente o tráfego de rede.

O recurso Imagem também está disponível diretamente da interface do programa em ESET Smart Security Business Edition e ESET NOD32 Antivirus Business Edition, ESET Endpoint Security ou ESET Endpoint Antivirus. Fica a critério do administrador qual será usado para implementar o servidor de Imagem.

Para ativar e iniciar o servidor de Imagem do ESET Smart Security Business Edition ou ESET NOD32 Antivirus Business Edition, siga estas etapas:

1) Instale o ESET Smart Security Business Edition , ESET NOD32 Antivirus Business Edition (cliente versão 4.X), ESET Endpoint Security ou ESET Endpoint Antivirus.
2) Na janela **Configuração avançada** (F5), clique em **Diversos** > **Licenças**. Clique em **Adicionar...**, procure o arquivo *.*lic* e clique em **Abrir**. Isso instalará a licença e permitirá a configuração do recurso Imagem.
3) Na ramificação **Atualizar**, clique em **Configuração...** e clique na guia **Imagem**.
4) Marque as caixas de seleção ao lado de **Criar imagem de atualização** e **Fornecer arquivos de atualização através do servidor HTTP interno**.
5) Insira o caminho de diretório completo na pasta (**Pasta para armazenar arquivos da imagem**) na qual os arquivos de atualização serão armazenados.
6) O **Nome de usuário** e **Senha** servem como dados de autenticação para estações de trabalho clientes tentando obter acesso à pasta Imagem. Na maioria dos casos, não é necessário preencher esses campos.
7) Deixe a Autenticação como **NENHUM**.
8) Selecione os componentes a serem obtidos por download (componentes para todas as versões de idioma que serão usados na rede devem ser selecionados). Os componentes serão exibidos somente se estiverem disponíveis de servidores de atualização da ESET.

OBSERVAÇÃO: para manter a funcionalidade ideal, recomendamos que você habilite o download e a obtenção de imagem dos componentes do programa. Se essa opção estiver desativada, somente o banco de dados de assinaturas de vírus será atualizado, não os componentes do programa. Se a Imagem for usada como parte do ERA, essa opção poderá ser configurada no ERAC na guia **Ferramentas** > **Opções do servidor...** > **Avançado** > **Editar configurações avançadas...** > **ESET Remote Administrator** > **ERA Server** > **Configuração** > **Imagem**. Habilite todas as versões de idioma do programa presentes em sua rede.

OBSERVAÇÃO: Para configurar a imagem para usar o protocolo HTTPS para as atualizações do cliente, vá para **ERAC** > **Ferramentas** > **Opções de servidor...** > guia **Avançado** > **Editar configurações avançadas...** > **ESET Remote Administrator** > **ERA Server** > **Configuração** > **Imagem** > **Protocolo** > **HTTPS**.

6.7 Outras configurações

Na guia **Outras configurações**, você pode configurar um endereço de servidor **SMTP** para usar ao enviar pacotes de instalação por email e um endereço de email do administrador, que será usado no email enviado pelo administrador. Se for necessário autenticação pelo servidor, especifique o nome de usuário e senha apropriados.

Observação: Você pode proteger as conexões selecionando um protocolo de segurança a partir do menu suspenso **Conexão segura**. Estão disponíveis **TLS**, **SSL** e **Auto**, onde o protocolo disponível é selecionado automaticamente.

Novos clientes

- **Permitir novos clientes** - quando essa opção for selecionada, novos clientes serão automaticamente adicionados à lista de clientes após sua primeira conexão ao ERA Server. Os clientes importados via replicação de outros servidores ERA serão adicionados à lista de clientes automaticamente durante a replicação.
- **Redefinir automaticamente sinalizador "Novo" para novos clientes** - quando novos clientes selecionados não forem sinalizados como novos automaticamente após sua primeira conexão ao ERAS. Para obter mais detalhes, consulte a descrição da guia **Clientes**.

Portas - permite que você personalize portas.

- **Console**: porta usada pelo ERA Console para se conectar ao ERA Server (por padrão, 2223).
- **Cliente**: porta usada pelo cliente da ESET para se conectar ao ERA Server (por padrão, 2222).
- **Porta de replicação deste servidor**: porta usada pelo ERA para replicação para um ERA Server superior (por padrão, 2846).
- **Instalador remoto da ESET (agente)**: porta usada pelo agente de instalação remota para instalação remota (Instalador remoto da ESET; por padrão, 2224).
- **Servidor da Web**: porta usada para conexão ao servidor da Web (por padrão, 2225).

OBSERVAÇÃO: para que alterações na configuração de porta sejam implementadas, o serviço ERA Server do NOD32 deve ser reiniciado.

ESET Live Grid

- **Coletando** - o ERAS encaminhará arquivos suspeitos e informações estatísticas de clientes para servidores da ESET em um intervalo de tempo especificado. Em alguns casos, não é possível coletar essas informações diretamente de clientes.

Painéis

- **Configurar lista de servidores da web...** - clique aqui para acessar a Lista de servidores da web de painel 41.

6.8 Avançadas

A guia **Avançadas** na janela **Opções do servidor** permite que você acesse e modifique as configurações avançadas do servidor através do Editor de configuração da ESET. Você pode abrir o Editor de configuração clicando no botão **Editar configurações avançadas...** nessa guia. Leia a mensagem de aviso e prossiga com atenção.

As configurações avançadas incluem as seguintes:

- **Uso máximo de espaço em disco (percentuais)** - quando excedido, alguns recursos do servidor podem não estar disponíveis. Ao se conectar ao ERAS, o ERAC exibirá uma notificação se o limite for excedido.
- **Codificação preferida de protocolo de comunicação** - define o tipo de codificação. Recomendamos a configuração padrão.
- **Permitir renomear endereço MAC (de desconhecido a válido)** - depois de instalar de uma solução cliente da ESET não compatível com o envio de um endereço MAC (p. ex., ESET NOD32 Antivirus 2.x) a uma solução cliente que é compatível (p. ex., um cliente 3.x), o registro de cliente anterior será convertido no novo. Recomendamos a configuração padrão (Sim).

- **Permitir renomear endereço MAC (de válido a desconhecido)** - depois de instalar de uma solução cliente da ESET compatível com o envio de um endereço MAC (p. ex., ESET NOD32 Antivirus 3.x) a uma solução cliente que é não compatível (p. ex., um cliente 2.x), o registro de cliente anterior será convertido no novo. Recomendamos a configuração padrão (Não).
- **Permitir renomear endereço MAC (de válido para outro válido)** - permite renomear endereços MAC válidos. O valor padrão não permite renomear, o que significa que o endereço MAC faz parte da identificação exclusiva de clientes. Desabilite essa opção se houver várias entradas para um PC. Além disso, recomendamos desabilitar essa opção se um cliente for identificado como o mesmo cliente depois de o endereço MAC ter sido alterado.
- **Permitir renomear nome do computador** - permite renomear computadores clientes. Se essa opção estiver desabilitada, o nome do computador fará parte da identificação exclusiva de clientes.
- **Usar logon padrão de servidor também por instalação forçada** - o ERAS permite que o usuário defina o nome de usuário e senha somente para script de logon e instalação remota por email. Habilite essa opção para usar os valores predefinidos também para instalações forçadas remotas.

7. Console da linha de comando ERA

O console da linha de comando ERA é uma ferramenta que permite executar tarefas e gerenciar clientes diretamente a partir da linha de comando, seja ao iniciar a ferramenta do Console da linha de comando ERA a partir da pasta onde está o Console ERA ou ao digitar *eracmd.exe* no prompt de comando.

Ao iniciar o Console da linha de comando ERA, será solicitado que você envie suas credenciais de login. Se este parâmetro ficar em branco, os valores padrão serão usados.

Observação: O Console da linha de comando ERA conta com a função auto completar. Comece a digitar um comando no console e pressione TAB para completar o comando. Pressionar TAB várias vezes passa por todas as opções disponíveis. Pressionar as setas UP/DOWN passa por todo o histórico de comandos inseridos. Pressionar ESC faz você voltar ao texto anterior, pressionar ESC duas vezes apaga completamente o texto.

Sintaxe a partir da linha de comando:

eracmd.exe --connectionparameters [command arguments [-commandflags]] [;command arguments -commandflags]

Exemplo:

eracmd.exe --s 127.0.0.1 version server -format csv

Depois de iniciado, o console da linha de comando ERA tenta automaticamente conectar ao servidor. Se a conexão for bem sucedida, o eracmd começa a processar os comandos. Se um comando não for especificado, o eracmd começa no modo shell, onde o usuário pode escrever comandos e ver o resultado diretamente. Para ver uma lista com os comandos disponíveis, digite o comando HELP COMMANDS.

Sintaxe no modo shell:

[command arguments [-commandflags]] [;command arguments -commandflags]

Para argumentos com espaços em branco, use aspas para colocar todas as palavras em um único argumento. Para deixar aspas dentro de um argumento deste tipo, use aspas duplas. Por exemplo, "Diga ""olá"" por favor" será interpretado como 'Diga "olá" por favor'

Duas palavras conectadas entre si (uma delas com aspas) serão conectadas. Por exemplo, "Diga "olá será interpretado como 'Diga olá'

Os comandos e palavras chave eracmd não diferenciam maiúsculas de minúsculas. Apenas argumentos usados para consultas no banco de dados podem diferenciar maiúsculas de minúsculas.

@-replacing:

Qualquer parte de um comando pode ser retirada de um arquivo. O caminho do arquivo deve ser cercado pelo símbolo @. Quando esta sintaxe for usada, o conteúdo do arquivo especificado é usado para tomar seu lugar. Se o arquivo tiver mais linhas, essas linhas são conectadas juntas com vírgulas e usadas como uma linha única. Assim, é possível salvar um arquivo com uma lista de argumentos que serão usados no próximo comando. Linhas vazias são ignoradas. Para suprimir este recurso, o símbolo @ deve ser cercado de aspas.

Exemplos:

O arquivo *myconnection.txt* contém o texto '*--s 192.168.0.1*' e depois o comando

eracmd.exe @myconnection@ show clients id where name *-like "*@*"*

será usado como *eracmd.exe --s 192.168.0.1 show clients id where name -like *@**

Este exemplo cria uma tarefa de configuração para clientes com a palavra "notebook" em seu nome:

show client id where client_name -like *Notebook* -out notebookID.txt -format csv -header none

task config c:\task_config_01.xml @notebookID.txt@

Comandos[110]:

Digite HELP COMMANDS no terminal para ver uma lista de comandos disponíveis, digite HELP <command> para ver instruções específicas para um determinado comando. Os comandos podem ter parâmetros obrigatórios e opcionais, que podem ser especificados usando uma palavra-chave. Parâmetros opcionais chamados por uma palavra-chave podem ser usados em qualquer ordem depois dos parâmetros obrigatórios serem determinados. Um comando começa logo depois dos parâmetros de conexão, sem a necessidade de um prefixo. Se nenhum comando estiver

presente na linha de comando, o eracmd será iniciado no modo shell. Vários comandos podem ser especificados em uma linha, para separar os comandos use um ponto e vírgula (;). Para executar um arquivo de script contendo vários comandos, use o comando SCRIPT <scriptFileName>. Em um arquivo de script, os comandos são separados por quebras de linha.

Sinalizadores de comando:

Sinalizadores de comando definem o comportamento geral de um comando, como o formato de saída ou a forma de lidar com erros. Sinalizadores de comando devem ser anexados depois de um comando e de seus argumentos para funcionar corretamente. Cada palavra-chave de sinalizador tem um traço (-) como prefixo. Para ver uma lista de sinalizadores, digite o comando HELP FLAGS.

Comentários:

Quando estiver no modo shell, os comentários podem ser usados em scripts ou em argumentos da linha de comando. Um comentário começa com # e continua até o final da linha atual. O separador de comando não termina um comentário. Se # for usado em uma sequência citada, ele não inicia um comentário e é usado como uma parte normal do texto citado.

Modo shell:

No modo shell, pressione TAB para ativar o auto completar sensível ao contexto. Use o comando HISTORY para ativar, desativar ou limpar o histórico de comando. Para escolher um comando a partir do histórico, use as setas UP e DOWN. Para reverter as mudanças feitas pelo TAB ou pelas setas UP/DOWN, pressione ESC.

Script de inicialização:

O script de inicialização é um arquivo com um comando executado automaticamente no início do modo shell.

O arquivo de script padrão está localizado em ProgramData (Todos os usuários\Dados de aplicativo) em ESET\Administrador Remoto ESET\Console\eracmd_startup.txt. Um caminho alternativo pode ser especificado usando o argumento --startup eracmd.exe (por exemplo, eracmd.exe --startup startup_script.txt).

O script não é executado como um sub-script separado (como a execução usando o comando "script"), e sim é executado como se os comandos forem digitados diretamente no console no modo shell (para que os sinalizadores definidos no script de inicialização usando o comando “set” continuem definidor no modo shell).

O comando "set save" pode ser usado para salvar os valores de sinalizador atuais no script de inicialização, substituindo o arquivo do script de inicialização se ele já existir.

Se um comando de saída for usado no script de inicialização, os comandos depois do comando de saída não serão executados, mas o eracmd.exe não vai sair do modo shell.

Estilos de formatação

Sinalizadores de cabeçalho e campo podem ser usados para especificar estilos de formatação:

- keyword - textos constantes são usados (adequado para um pós-processamento automático_

- pretty - textos traduzíveis são usados (adequado para saída do usuário)

Os sinalizadores de cabeçalho afetam os cabeçalhos das tabelas (nomes de coluna). Sinalizadores de campo afetam os valores de campo das tabelas.

Parâmetros de conexão

Parâmetros que pertencem a uma conexão no servidor ERA devem ser especificados como parâmetros da linha de comando. O eracmd.exe processa comandos apenas se a conexão for estabelecida com sucesso. Todos os parâmetros de conexão usam o prefixo de traço duplo (--).

--s server:port: Servidor ao qual conectar. Valor padrão: localhost:2226
--u username: Nome de usuário do servidor ERA. Se o nome de usuário começar com um prefixo de domínio, ele será usado como um nome de usuário de autenticação de domínio. Este comando não pode ser usado combinado com o --ud ou --uc. Valor padrão: Administrator
--ud username: Nome de usuário de autenticação do domínio. Não pode ser usado combinado com o --u ou --uc.
--uc: Usa as credenciais de sessão do Windows atual. Não pode ser usado combinado com o --u ou --ud.
--p password: Senha de autenticação do servidor ERA ou domínio. Não pode ser usado combinado com o --pa. Valor padrão: "" (senha em branco).
--pa: Solicita uma senha. Depois de iniciar o console, será possível inserir uma senha exibindo apenas *. Não pode ser usado combinado com o --p.
--aa: Pede todos os parâmetros de conexão. Se for especificado, nenhum outro parâmetro de conexão pode ser especificado.
--startup: Caminho alternativo do script de inicialização. O script de inicialização é executado automaticamente no início do modo shell.

7.1 Sinalizadores de comando

Os sinalizadores podem ser usados para definir alguns comportamentos genéricos de comando ou para especificar a saída de cada comando. Para definir o valor padrão de cada sinalizador, use o comando SET. Os sinalizadores são inseridos depois de um comando e de seus argumentos. A seguir, há uma lista de sinalizadores disponíveis.

- *-format* : Formato de saída. Valores possíveis: *csv*, *table*. Valor padrão: *csv* (no modo da linha de comando), *table* (no modo shell).
- *-delim* : Delimitados da saída CSV. Se for usado com o argumento "", o delimitador do sistema será usado (que também é o valor padrão). Se um delimitador do sistema não for configurado, ',' será usado. Como o ponto e vírgula é usado como separador de comando, use as aspas para especificar o ponto e vírgula como um delimitador. Valor padrão: "" (delimitador do sistema, ',' se não estiver definido).
- *-out* : Redireciona a saída para um arquivo. Consulte também os sinalizadores -mode e -enc. Se for usado com o argumento "", o redirecionamento será desativado (que também é o comportamento padrão). Valor padrão: "" (encaminhamento desativado).
- *-mode* :Modo de saída do arquivo. Valores possíveis: o (substituir o arquivo), a (anexar no fim do arquivo). Valor padrão: o (substituir o arquivo).
- *-enc* : Codificação de saída do arquivo. Valores possíveis: *ansi*, *utf8*, *utf16*. Valor padrão: *utf8*.
- *-header* : Tipo de cabeçalho da tabela. Valores possíveis: *keyword* (usa palavras chave como as usadas nos argumentos de comando, por exemplo client_name), *pretty* (usa nomes de coluna mais legíveis e traduzíveis, por exemplo Nome do cliente), *none* (o cabeçalho não é exibido). Valor padrão: *keyword*.
- *-paged* : Saída por página. Se estiver ativado, o usuário é solicitado a pressionar uma tecla depois de cada página. Valores possíveis: *true*, *false*. Valor padrão: *false*.
- *-tableclip* : Corta a tabela para que ela caiba na tela. Isto é aplicado apenas ao produzir uma tabela para uma janela do console. Valores possíveis: *true*, *false*. Valor padrão: *true*.
- *-cor* : Use várias cores ao exibir o conteúdo na janela de console. Valores possíveis: *true*, *false*. Valor padrão: *true*.
- *-field* : Estilo de formatação do campo de tabela. Valores possíveis: *keyword* (usa palavras chave constantes, por exemplo finished_with_warning), *pretty* (usa textos mais legíveis e traduzíveis, por exemplo "Concluído com aviso"). Valor padrão: keyword.
- *-onerror* : O que fazer se um erro acontecer durante a execução de um comando. Se estiver definido para parar, a execução de uma sequência de comando vai parar imediatamente. Se estiver definido para configurar, a execução continua com os comandos seguintes. Toda a sequência termina com um status de erro se qualquer comando tiver falhado. Valores possíveis: *stop*, *continue*. Valor padrão: *stop*.

7.2 Comandos

COMANDO	DESCRIÇÃO	SINTAXE	PARÂMETROS	EXEMPLO
client comment	Define o comentário de cliente.	client comment <client ID> <comment>	**client ID** ID do cliente para o qual o comentário será definido. **comment** Comentário para o cliente.	client comment 1 Problematic
client new	Definir ou redefinir o sinalizador "novo" para um cliente no servidor.	client new <client ID> <action>	**client ID** Lista separada por vírgula dos IDs de clientes para definir ou redefinir o sinalizador "novo". **action** Se for definir ou redefinir o sinalizador "novo". Valores possíveis: set, reset	client new 1 reset
client rename	Renomeia um cliente no servidor.	client rename <client ID> <name>	**client ID** ID do cliente a ser renomeado. **name** Novo nome do cliente.	client rename 1 new_client_name
client roaming	Definir ou redefinir o sinalizador "usuário em roaming" para um cliente no servidor.	client roaming <client ID> <action>	**client ID** Lista separada por vírgula dos IDs de clientes para definir ou redefinir o sinalizador "usuário em roaming". **action** Se for definir ou redefinir o sinalizador "usuário em roaming". Valores possíveis: set, reset	client roaming 1 set
cls	Limpa a saída do console.	cls		cls
echo	Exibe um argumento como mensagem. Se o argumento estiver faltando, apenas uma nova linha é inserida na saída.	echo [<message>]	**message** Mensagem a ser exibida. Pode conter valores múltiplos concatenados.	echo "hello world" echo "Report created with id: ",@reportId.csv@ echo

encrypt	Criptografa uma senha para ser usada na configuração. Dois tipos de criptografia são usados: "servidor", que é usado para senhas definidas pelo servidor era (replicação, cliente, instalador, usuários), e "outros", que é usado para senhas definidas por outros serviços (smtp, atualização, ...). O resultado é que este comando exibe a senha criptografada, que pode ser usada para criar arquivos de configuração. Se uma senha não for especificada, o usuário será solicitado a inserir a senha e os caracteres no campo de senha serão exibidos como asteriscos.	encrypt <encryptionType> [<password>]	**encryptionType** Tipo de criptografia. Valores possíveis: server, other **password** Senha a ser criptografada.	encrypt server MyReplicationPassword6578
errmsg	Exibe uma mensagem de erro para um código de erro.	errmsg <code>	**code** Código de erro a ser visualizado relacionado a uma mensagem de erro.	errmsg 2001
exit	Finaliza o console da linha de comando se for usado a partir do modo shell. Para a execução do arquivo de script se for usado em um arquivo de script.	exit		

getdata	Obtém o conjunto de informações especificado a partir de um cliente em particular ou em relação a uma política em particular para um arquivo local. Algumas informações podem estar indisponíveis no servidor, para atualizar as informações use o comando REQUEST. Configuração, Recursos de proteção, Status da proteção e Informações sobre o sistema são atualizados automaticamente para clientes no servidor primário.	getdata <data type> <data ID> <file>	**data type** Tipo de dados a serem obtidos. Valores possíveis: Cliente: sysinspector (Relatório do SysInspector), configuration (Configuração XML), protection_status (Status da proteção), protection_features (Recursos de proteção), system_information (Informações do sistema); Política: policy (Política XML, apenas para políticas não replicadas a partir do servidor superior), policy_merged (Política Mesclada XML, criada como resultado de uma herança ao aplicar as configurações da política superior), policy_override (Substituição de Política Parte XML, apenas para políticas replicadas a partir do servidor superior), policy_nonoverride (Política Sem Substituição Parte XML) **data ID** ID da entidade de dados (cliente ou política) da qual fazer download dos dados. **file** Caminho de arquivo do local de destino.	getdata configuration 1 c:\file.xml
group	Exibe grupos definidos e informações de grupos.	group [<tree>]	**tree** Usa o modo em árvore para exibir os grupos com a herança do grupo.	group
help	Exibe informações sobre usar o Console da linha de comando ERA. Use o argumento para selecionar uma ajuda mais especializada.	help [<command 1>] [<command 2>]	**command 1** Comando pelo qual exibir a ajuda (primeira palavra do nome de um comando). Valores possíveis: <command name>, flags, commands **command 2** Comando pelo qual exibir a ajuda (segunda palavra do nome de um comando).	help version help commands help help

history	Ativa ou desativa o histórico de comando de salvar persistente do modo shell depois de sair do console. O padrão está desativado.	history [<action>]	**action** Se for omitido, o estado atual do histórico de salvar depois de sair do console será exibido. Valores possíveis: true (ativar), false (desativar), clean (apaga o histórico do comando), list (exibe conteúdo atual do histórico salvo)	history true
license	Exibe as informações de licença do servidor.	license		license
license add	Faz o upload do arquivo ou arquivos da chave de licença especificada para o servidor ERA.	license add <filename>	**filename** Lista separada por vírgula dos caminhos de arquivos da chave de licença para fazer upload.	license add c:\era.lic
license details	Exibe informações sobre chaves de licença parciais carregadas pelo servidor ERA.	license details		license details
license replace	Faz o upload de um arquivo ou arquivos da chave de licença para o servidor ERA e substitui todos os arquivos de licença anteriores pelas chaves de licença enviadas.	license replace <filename>	**filename** Lista separada por vírgula dos caminhos de arquivos da chave de licença para substituir.	license replace c:\era.lic

logforward	Exibe ou define as configurações atuais de encaminhamento de relatório. Há duas maneiras de usar este comando: 1. Para exibir o estado de uma configuração de encaminhamento de relatório em particular, use o primeiro parâmetro <type> ou use o comando sem nenhum parâmetro para exibir as configurações de encaminhamento de relatório atuais de todos os relatórios. 2. Para definir configurações de encaminhamento de registro, os parâmetros <type> e <enable> são obrigatórios. Outros parâmetros ([nível <level>], [gravidade <severity>] e [recurso <facility>]) são opcionais. Se um parâmetro opcional for omitido, o valor continuará inalterado.	logforward [<type>] [<enable>] [level <level>] [severity <severity>] [facility <facility>]	**type** Tipo de relatório a ser exibido ou atualizado. Valores possíveis: event, threat, firewall, hips, antispam, greylist, scan, mobile, device_control, web_control **enable** Determina se o encaminhamento deve estar ativado ou desativado. Valores possíveis: true, false **level** Nível do relatório a ser processado pelo encaminhamento de relatório. Valores possíveis: critical, warning, normal, diagnostics **severity** Valor de gravidade do SysLog. Valores possíveis: informational, error, warning, debug **facility** Valor de recurso do SysLog. Valores possíveis: 0 a 23	logforward logforward scan logforward eventlog true level warning logforward threat false
password	Altera uma senha de segurança do servidor ERA. Para uma senha em branco, use "". Se as senhas antigas e novas não forem especificadas, o usuário será solicitado a inserir a senha, as senhas digitadas serão exibidas como asteriscos. Este comando não pode definir senhas que sejam parte da configuração do servidor. Para essas senhas use o comando SERVERCFG SET ou SERVERCFG SETPWD.	password <passwordType> [<oldPassword> <newPassword>]	**passwordType** Tipo de senha a ser definida. Valores possíveis: replication, client, installer, currentuser **oldPassword** Senha antiga. É possível usar uma senha de administrador de servidor ERA. **newPassword** Nova senha.	password currentuser password replication oldPass1 newPass2

path	Exibe ou define o diretório de trabalho atual usado como base para todos os caminhos relativos (ao especificar o caminho de script ou os caminhos de arquivos de dados).	path [<action>] [<path>]	**action** Ação. Valores possíveis: get (exibe o diretório de trabalho atual), set (define o caminho especificado como o próximo argumento), script (define para o caminho do script atual). Valor padrão: get **path** Novo diretório de trabalho. Se for um caminho relativo, ele é considerado relativo ao diretório de trabalho anterior.	path path set d:\scripts path script
policy	Exibe políticas definidas com informações de política. Se o argumento "tree" estiver presente, exibe uma árvore de hierarquia das políticas.	policy [<tree>]	**tree** Usa o modo em árvore para exibir as políticas com a herança de política.	policy policy tree
policy assign	Atribui uma política especifica aos clientes especificados. Note que não é possível atribuir qualquer política para qualquer cliente. Se a lista de cliente tiver clientes replicados, a política deve poder ser replicada para baixo. Políticas de servidores de baixo não podem ser atribuídas.	policy assign <policy id> <clients>	**policy id** A política atribuída. Valores possíveis: <policy ID>, ! DefaultClientsPolicy **clients** Lista separada por vírgula dos IDs de cliente (ou * para todos os clientes).	policy assign 10 1,2,5,9 policy assign ! DefaultClientsPolicy *

policy create	Cria uma política dentro dos parâmetros especificados no servidor. Exibe o ID da nova política, se ela for criada com sucesso.	policy create <name> <config XML> [parentID <parent ID>] [description <description>] [overrideAnyChild <override any child>] [downReplicable <down replicable>] [defaultForClients <default for clients>] [defaultForLowerServers <default for lower servers>]	**name** Nome da nova política. **config XML** Arquivo XML com a configuração da nova política. **parent ID** ID do pai da nova política. **description** Descrição da nova política. **override any child** Define o sinalizador "Substituir qualquer política filha" para a nova política. Valores possíveis: true, false. Valor padrão: false **down replicable** Define o sinalizador "Política replicável para baixo" para a nova política. Valores possíveis: true, false. Valor padrão: false **default for clients** Define a política como política padrão para clientes. Valores possíveis: true, false. Valor padrão: false **default for lower servers** Define a política como política padrão para servidores inferiores. Valores possíveis: true, false. Valor padrão: false	policy create new_policy policy.xml

policy delete	Exclui uma política e permite que você defina substituições para a política excluída. Substituições desnecessárias são ignoradas.	policy delete <policy id> [child_policies <child policies parent replacement>] [primary_clients <primary clients policy replacement>] [replicated_clients <replicated clients policy replacement>] [primary_clients_default <primary clients default policy replacement>] [lower_servers_default <lower servers default policy replacement>] [whole_branch <delete whole branch>]	**policy id** ID da política a ser excluída. **child policies parent replacement** Nova política pai para as políticas filho da política atualmente excluída. Valores possíveis: <policy ID>, ! DefaultUpperServerPolicy, !Not Available **primary clients policy replacement** Nova política para clientes primários com a política atualmente excluída. Valores possíveis: <policy ID>, ! DefaultClientsPolicy **replicated clients policy replacement** ID da nova política para clientes replicados com a política atualmente excluída. **primary clients default policy** ID de substituição da nova política padrão para clientes primários. **lower servers default policy** Nova política padrão para servidores inferiores. Valores possíveis: <policy ID>, ! NotAvailable **delete whole branch** Se toda a ramificação (a política especificada, incluindo políticas filhas) tiver que ser excluída. Valores possíveis: true, false Valor padrão: false	policy delete 2 primary_clients 4
rule	Exibir regras de política.	rule		rule

rule create	Cria uma nova regra de política	criar regra <xml> <name> <policy id> [descrição <description>] [prioridade <priority>] [ativado <enable>]	**xml** Arquivo XML de origem, criado ao exportar a regra existente. **name** Nome da regra da política. **policy id** ID da política relacionada. Apenas os tipos a seguir podem ser usados: política padrão de clientes, políticas locais, políticas replicáveis para baixo a partir do servidor superior. Valores possíveis: , ! DefaultClientsPolicy **description** Descrição da regra da política. **priority** Prioridade da regra da política. Valores possíveis: top, bottom Valor padrão: bottom **enable** Estado inicial da regra de política criada. Valores possíveis: true, false Valor padrão: true	rule create "c:\my data\exportedPolicy.xml" myNewPolicy 3 desc "New policy rule" priority top enabled false
rule delete	Exclui uma regra de política	excluir regra <policy rule id>	**policy rule id** ID da regra de política a ser excluída.	rule delete 3
rule import	Importa as regras de política a partir de um arquivo XML. As regras já definidas não serão alteradas. Se o nome de uma regra já existir, a nova regra (importada) será renomeada.	importar regra <file path>	**file path** Caminho de arquivo XML de onde importar as regras.	rule import d:\rule.xml
rule export	Exportar as regras de política para um arquivo XML.	exportar regra <rules> <file path>	**rules** Lista separada por vírgula de IDs das regras (ou * para todas as regras). **file path** Caminho de arquivo XML para onde importar as regras.	rule export 1,2 d:\rule.xml

rule update	Alterar parâmetro ou configurações de uma regra de política. Parâmetros não especificados continuarão sem ser alterados.	atualização de regra <policy rule id> [xml <config xml>] [descrição <description>] [política <policy id>] [prioridade <priority>] [ativado <enable>]	**policy rule id** ID da regra de política a ser atualizada. **config xml** Configuração do arquivo XML criado ao exportar a regra existente. **description** Nova descrição da regra de política.. **policy id** Nova ID da política relacionada. Valores possíveis: , ! DefaultClientsPolicy **priority** Alteração de prioridade da regra de política. Valores possíveis: up, down, top, bottom **enable** Novo estado da regra de política. Valores possíveis: true, false	rule update 2 xml d:\rule.xml enabled true

policy update	Atualiza uma configuração de política com os parâmetros especificados.	policy update <ID> [name <name>] [parentID <parent ID>] [configXML <config XML>] [description <description>] [overrideAnyChild <override any child>] [downReplicable <down replicable>] [defaultForClients <default for clients>] [defaultForLowerServers <default for lower servers>] [replicated_clients <replicated clients policy replacement>] [lower_servers_default <lower servers default policy replacement>] [primary_clients_default <primary clients default policy replacement>]	**ID** ID da política atualizada. **name** Novo nome da política atualizada. **parent ID** Novo ID da política pai da política atualizada. Valores possíveis: <policy ID>, ! NoPolicy (a política atualizada não terá pai) **config XML** Arquivo XML com a nova configuração da política atualizada. **description** Nova descrição da política atualizada. **override any child** Novo valor do sinalizador "Substituir qualquer política filha" para a política atualizada. Valores possíveis: true, false **down replicable** Novo valor do sinalizador "Política replicável para baixo" para a política atualizada. Valores possíveis: true, false **default for clients** Define a política como política padrão para clientes. Valores possíveis: true, false **default for lower servers** Define a política como política padrão para servidores inferiores. Valores possíveis: true, false **replicated clients policy replacement** Nova política para clientes replicados com a política atualmente atualizada. Valores possíveis: <policy ID>, ! DefaultClientsPolicy, ! NotAvailable	policy update 123 name policy1 parentID 1 configXML policy.xml overrideAnyChild TRUE defaultForLowerServers FALSE

			lower servers default policy replacement Nova política padrão para servidores inferiores. Valores possíveis: <policy ID>, ! DefaultClientsPolicy, ! NotAvailable **primary clients default policy replacement**ID da nova política padrão para clientes primários.	
report	Exibe os modelos de relatório estáticos ou de painel ou os relatórios gerados. No caso de relatórios gerados, apenas os relatórios localizados no servidor são exibidos.	report <type>	**type** Tipo de relatório. Valores possíveis: static, dashboard, generated	report static
request	Solicita que a versão atual de vários dados seja transferida de um cliente para o servidor ERA. É possível solicitar informações do SysInspector, Configuração, Status da Proteção, Recursos de Proteção e Informações sobre o sistema. Os dados solicitados serão recebidos assim que o cliente conectar no servidor primário e os dados estiverem disponíveis. Em clientes replicados, primeiro a solicitação precisa ser replicada. Configuração, Recursos de proteção, Status da proteção e Informações sobre o sistema são atualizados automaticamente para clientes no servidor primário.	request <data type> <clients> [si_compare <compare date>] [<si_snapshot>]	**data type** Lista separada por vírgula de tipos de dados a serem solicitados. Valores possíveis: sysinspector, configuration, protection_status, protection_features, system_information **clients** Lista separada por vírgula dos IDs de cliente (ou * para todos os clientes). **compare date** Se for usado, compara o relatório solicitado com um relatório anterior especificado por data e hora em UTC no formato AAAA-MM-DD hh:mm:ss (por exemplo "2014-01-21 10:43:00"). Usado apenas ao solicitar Informações do SysInspector. **si_snapshot** Salva o relatório de forma local na estação de trabalho do cliente. Usado apenas ao solicitar Informações do SysInspector.	request protection_features * request sysinspector,config 1,2,8 si_compare "2014-01-01 01:02:03" si_snapshot
scanlog	Exibe o conteúdo do relatório de rastreamento especificado.	scanlog <id>	**id** ID de um relatório de rastreamento solicitado.	scanlog 1
script	Executa um lote de comandos em um	script <filename>	**filename** Caminho para o arquivo com os	script c:\eraGetClientsInfo.txt

	arquivo externo.		comandos. Os comandos podem ser separados por uma nova linha ou por um ponto e vírgula.	
servercfg get	Faz o download da configuração atual do servidor para o arquivo local especificado.	servercfg get <filename>	**filename** Caminho de arquivo local para onde salvar a configuração baixada.	servercfg get d:\era_config.xml
servercfg list	Exibe as definições de configuração disponíveis que podem ser modificadas diretamente pelos comandos SERVERCFG SET e SERVERCFG SETPWD.	servercfg list		servercfg list
servercfg put	Atualiza a configuração do servidor de um arquivo XML local.	servercfg put <filename>	**filename** Caminho de arquivo XML local a ser enviado.	servercfg put d: ew_config.xml
servercfg set	Atribui um valor a uma definição de configuração em particular. Use o comando HELP SERVERCFG LIST para exibir todas as configurações disponíveis.	servercfg set <name=value>	**name=value** Nome da configuração e o valor a ser atribuído.	servercfg set port_con=2223 servercfg set mirror_enabled=1
servercfg setpwd	Atribui um valor a uma definição de configuração em particular através de um prompt por senha. Os valores digitados são exibidos como asteriscos, portanto isto é útil para inserir senhas. Use o comando HELP SERVERCFG LIST para exibir todas as configurações disponíveis. Este comando não pode definir as senhas de segurança do servidor, use o comando PASSWORD para isto.	servercfg setpwd <name>	**name** Nome da configuração a ser definida.	servercfg setpwd ps_password_smtp

set	Obtém, define ou salva os valores dos sinalizadores. Sinalizadores são usados para especificar a saída de comando e outras configurações comuns. Para ver uma lista de todos os sinalizadores disponíveis, use o comando HELP FLAGS. Configurar um sinalizador tem efeito para todos os comandos subsequentes no arquivo de script atual ou para todos os comandos subsequentes no modo shell (se for usado diretamente no modo shell). O sinalizador pode ser substituído por um comando único especificando um sinalizador de comando depois do comando.	set [<flag name>] [<flag value>]	**flag name** Use o nome do sinalizador sem o traço inicial. Use o comando HELP FLAGS para ver uma lista de sinalizadores disponíveis. Se não for especificado, os valores atuais para todos os sinalizadores são impressos. Alternativamente, é possível usar o “save” para salvar o estado dos sinalizadores atuais no arquivo de inicialização (use o segundo argumento para especificar um caminho de arquivo de inicialização alternativo). **flag value** Use o comando HELP FLAGS para ver os valores disponíveis. Se não for especificado, o valor atual do sinalizador é impresso.	set set enc set enc utf8 set format table set paged true set save set save startup.txt
show	Exibe dados para a tabela específica. Use "count" no lugar de uma lista de colunas para obter apenas a contagem de fileiras.	show <table name> <list of columns> [where <where>] [group by <group by>] [order by <order by>] [skip <skip>] [limit <limit>]	**table name** Use o comando SHOW TABLES para ver as tabelas disponíveis. **list of columns** Lista separada por vírgula. Use o comando SHOW COLUMNS para ver uma lista de colunas para a tabela em específico. Use * para todas as colunas. Use "count" para obter apenas a contagem de fileiras. Valores possíveis: <column name>, *, contagem com uma lista separada por vírgula das condições no formato <column><comparison operator><value> (e.g. id>3) ou <column> <IN operator> (<comma_separated_values_list>). Os operadores de comparação seguintes são permitidos: = (ou -EQ), != (ou -NE), <= (ou -LE), >= (ou -GE), < (ou -LT), > (ou -GT). Os	show client * show client client_name show client id, client_name WHERE id>4, configuration -IN (ready, requested) ORDER BY client_name LIMIT 5 show client * WHERE product_name -LIKE *endpoint* show client count WHERE id>4 show client * where group_id=4 show client * where requested_policy_id -IN (2,3) show event * where client_group_id=4 show event * where client_requested_policy_id -IN (2,3)

			operadores IN seguintes são permitidos: -IN ou -NOTIN. Para colunas de texto, -LIKE e -NOTLIKE com um valor de texto com caracteres curinga (* - zero ou mais caracteres, ? - exatamente um caractere) podem ser usados no lugar de um operador de comparação. **group by** Lista separada por vírgula das colunas de acordo com as quais fazer o agrupamento. Fileiras com os valores correspondentes em todas essas colunas serão exibidas como uma fileira. **order by** Lista separada por vírgula das colunas de acordo com as quais ordenar. Depois de cada nome de coluna, -ASC (padrão) ou -DESC podem ser especificados para ordem crescente ou decrescente. **skip** Quantas fileiras pular no início. **limit** Contagem máxima de fileiras a serem exibidas.	
show columns	Exibir colunas disponíveis para a tabela especificada.	show columns [for] <table name>	**table name** Tabela para a qual exibir as colunas. Use o comando SHOW TABLES para obter os nomes disponíveis de tabelas.	show columns for client
show tables	Exibe as tabelas disponíveis que podem ser usadas no comando SHOW.	show tables		show tables
task config	Cria uma tarefa de configuração ao usar um arquivo de configuração. Exibe o ID da nova tarefa, se ela for criada com sucesso.	task config <configuration file> <clients> [name <name>] [description <description>] [applyAfter <apply after>] [deleteIfCompleted <delete if completed>]	**configuration file** Arquivo XML do editor de configuração. **clients** Lista separada por vírgula dos IDs de cliente (ou * para todos os clientes). **name** Nome da tarefa.	task config d:\task_config_01.xml 1,4,5 name "Config01" description "email client protection config"

			description Descrição da tarefa. **apply after** Hora UTC quando a tarefa vai ter que ser aplicada, em um dos formatos a seguir: AAAA-MM-DD hh:mm:ss, AAAA-MM-DD hh:mm, AAAA-MM-DD hh, AAAA-MM-DD. Por exemplo (data com hora): "2014-01-21 10:43". Exemplo (data sem hora): "2014-01-21". **delete if completed** Use se a tarefa tiver que ser excluída depois de ser concluída com sucesso. Valores possíveis: true, false. Valor padrão: false.	
task scan	Cria uma tarefa de rastreamento. Exibe o ID da nova tarefa, se ela for criada com sucesso.	task scan <clients> [name <name>] [description <description>] [applyAfter <apply after>] [deleteIfCompleted <delete if completed>] [exclude <exclude>] [windows_profile <profile>] [windows_targets <windows targets>] [windows_no_cleaning <no cleaning>] [windows_shutdown_after_scan <shutdown>] [windows_allow_shutdown_cancel <allow cancel>] [linux3_targets <linux3 targets>] [linux3_no_cleaning <no cleaning>] [linux_profile <profile>] [linux_targets <linux targets>] [linux_no_cleaning <no cleaning>] [mobile_targets <mobile targets>] [mobile_no_cleaning <no cleaning>] [max_delay <max delay>]	**clients** Lista separada por vírgula dos IDs de cliente (ou * para todos os clientes). **name** Nome da tarefa. **description** Descrição da tarefa. **apply after** Hora UTC quando a tarefa vai ter que ser aplicada, em um dos formatos a seguir: AAAA-MM-DD hh:mm:ss, AAAA-MM-DD hh:mm, AAAA-MM-DD hh, AAAA-MM-DD. Por exemplo (data com hora): "2014-01-21 10:43". Exemplo (data sem hora): "2014-01-21". **delete if completed** Se a tarefa tiver que ser excluída depois de ser concluída com sucesso. Valores possíveis: true, false. Valor padrão: false. **exclude** Lista separada por vírgula de seções a serem excluídas da tarefa de rastreamento. Valores possíveis: windows, linux3, linux, mobile. **profile** Nome do perfil de rastreamento. Valores possíveis: !	task scan 1,3

			InDepthScan, !MyProfile, !SmartScan, !ContextMenuScan, <user-defined profile name>. Valor padrão: !InDepthScan **windows targets** Lista separada por vírgula de alvos do Windows para rastreamento. Valores possíveis: !Memory, !RemovableDrivesBoot, !RemovableDrives, !LocalDrivesBoot, !LocalDrives, !RemoteDrives, !AllDrivesBoot, !AllDrives, <custom path> Valor padrão: !Memory, !LocalDrivesBoot, !LocalDrives **no cleaning** Rastrear sem limpar. Valores possíveis: true, false. Valor padrão: false **shutdown** Desligar computador depois do rastreamento. Valores possíveis: true, false. Valor padrão: false **allow cancel** Permitir que um usuário cancele o desligamento. Valores possíveis: true, false. Valor padrão: false **linux3 targets** Lista separada por vírgula de caminhos do linux3 para rastreamento. Valor padrão: / **linux targets** Lista separada por vírgula de caminhos do linux para rastreamento. Valor padrão: / **mobile targets** Lista separada por vírgula de alvos móveis para rastreamento. Valores possíveis: !All, <custom path> Valor padrão: !All **max delay** Atraso aleatório máximo em minutos.	

task update	Cria uma tarefa de atualização. Exibe o ID da nova tarefa, se ela for criada com sucesso.	task update <clients> [name <name>] [description <description>] [applyAfter <apply after>] [deleteIfCompleted <delete if completed>] [exclude <exclude>] [windows_profile <windows profile>] [max_delay <max delay>]	**clients** Lista separada por vírgula dos IDs de cliente (ou * para todos os clientes). **name** Nome da tarefa. **description** Descrição da tarefa. **apply after** Hora UTC quando a tarefa vai ter que ser aplicada, em um dos formatos a seguir: AAAA-MM-DD hh:mm:ss, AAAA-MM-DD hh:mm, AAAA-MM-DD hh, AAAA-MM-DD. Por exemplo (data com hora): "2014-01-21 10:43". Exemplo (data sem hora): "2014-01-21". **delete if completed** Use se a tarefa tiver que ser excluída depois de ser concluída com sucesso. Valores possíveis: true, false. Valor padrão: false **exclude** Lista separada por vírgula de seções a serem excluídas da tarefa de atualização. Valores possíveis: windows, linux3, linux, mobile **windows profile** Nome do perfil para a seção do windows. **max delay** Atraso aleatório máximo em minutos.	task update 2,4,6 name "Update01" exclude windows task update *
version	Exibe a versão atual do Console da linha de comando, API e Servidor ERA.	version [<component>]	**component** Qual versão de componente deve ser exibida. Se estiver faltando, todas as versões são exibidas. Valores possíveis: cmd, api, server	version version cmd

8. ERA Maintenance Tool

A finalidade da ESET Remote Administrator Maintenance Tool é executar tarefas específicas de operação e manutenção do servidor. Ele pode ser acessado clicando-se em **Iniciar** > **Programas** > **ESET** > **ESET Remote Administrator Server** > **ESET Remote Administrator Maintenance Tool**. Quando você iniciar a ERA Maintenance Tool, um assistente interativo será exibido para ajudá-lo a realizar as tarefas necessárias.

Depois que iniciar a ESET Remote Administrator Maintenance Tool e clicar em **Avançar**, você poderá ver a janela de informações do ERA Server. A ferramenta exibirá informações de resumo sobre o ERA Server instalado. As informações exibidas poderão ser visualizadas em mais detalhes em uma janela separada clicando-se em **Mais informações**. Elas poderão ser copiadas clicando-se em **Copiar para a área de transferência** e poderão ser atualizadas clicando-se em **Atualizar**. Depois de verificar as informações, prossiga para a próxima etapa clicando em **Avançar** e selecione uma tarefa:

- Parar o ERA Server 128
- Iniciar o ERA Server 128
- Transferência do banco de dados 129
- Backup do banco de dados 129
- Restauração do banco de dados 130
- Excluir tabelas 130
- Backup de armazenamento 130
- Restauração de armazenamento 130
- Instalar nova chave de licença 131
- Modificar configuração do servidor 131

Ao final de cada configuração de tarefa, você poderá salvar as configurações da tarefa atual clicando em **Salvar todas as configurações em arquivo**. As configurações poderão então ser usadas a qualquer momento no futuro clicando-se em **Carregar todas as configurações do arquivo**. Cada etapa individual em uma configuração de tarefa também terá a opção de **Salvar todas as configurações em arquivo** ou **Carregar todas as configurações do arquivo**.

8.1 Parar o ERA Server

Essa tarefa interromperá o serviço do ESET Remote Administrator Server.

OBSERVAÇÃO: o nome do serviço é ERA_SERVER. O executável para esse serviço é "C:*Program Files**ESET**ESET Remoto Administrator**Server**era.exe*".

8.2 Iniciar o ERA Server

Essa tarefa iniciará o serviço do ESET Remote Administrator Server.

OBSERVAÇÃO: o nome do serviço é ERA_SERVER. O executável para esse serviço é "C:*Program Files**ESET**ESET Remote Administrator**Server**era.exe*".

8.3 Transferência do banco de dados

Esta tarefa permitirá que você converta o formato do banco de dados. A ferramenta pode converter entre os seguintes bancos de dados:

- MS Access
- MS SQL Server
- Oracle
- MySQL

A primeira etapa é verificar a conexão do banco de dados. Essa etapa é comum para todas as tarefas, exceto ao carregar uma nova chave de licença e modificar a configuração do servidor.

Se o banco de dados for um banco de dados do MS Access, especifique o caminho para o arquivo *.mdb*. Por padrão, é usado o caminho especificado durante a instalação do ERA Server.

Todos os outros formatos de banco de dados exigem que parâmetros adicionais sejam definidos:

- Cadeia de caracteres de conexão: cadeia de caracteres especial para identificar o banco de dados de origem
- Usuário: nome de usuário para acessar o banco de dados
- Senha: senha para acessar o banco de dados
- Nome do esquema: nome de um esquema (disponível somente para Oracle e MS SQL)

Clique em **Carregar configuração do servidor atual** para usar as atuais configurações do ERA Server. Para testar a conexão do banco de dados, clique em **Testar conexão**. Se a conexão não puder ser estabelecida, verifique os parâmetros quanto a erros. Depois que o teste do banco de dados for bem-sucedido, continue clicando em **Avançar**.

Em seguida, selecione o banco de dados de destino. Selecione **Substituir configurações de conexão do servidor** para conectar o servidor e usar o novo banco de dados depois da conversão bem-sucedida. Não selecionar essa opção fará com que o novo banco de dados seja criado sem o servidor ser atualizado para a nova versão do banco de dados.

Para todos os tipos de banco de dados, além do banco de dados do MS Access, selecione se deseja criar as tabelas de banco de dados automaticamente (**Criar tabelas automaticamente no banco de dados**) ou inserir as tabelas no banco de dados posteriormente (**Visualizar script** > **Salvar em arquivo**) na próxima etapa. Para um banco de dados do MySQL, a opção **Criar um novo banco de dados ESETRADB automaticamente** criará automaticamente um novo banco de dados do MS SQL nomeado ESETRADB. A etapa final é confirmar a conversão do banco de dados.

8.4 Backup do banco de dados

Esta ferramenta permitirá que você crie um arquivo de backup do banco de dados. As configurações na primeira janela são semelhantes àquelas na conversão do banco de dados (consulte o capítulo Transferência do banco de dados 129); nesta janela, o banco de dados de origem será selecionado. O banco de dados de origem será copiado em um arquivo de backup especificado na próxima etapa.

Parâmetros opcionais na parte inferior da janela permitem que você substitua o arquivo existente (**Substituir se houver**), bem como interrompa o ESET Remote Administrator Server durante o processo de backup (**Interromper servidor durante o processamento da tarefa**). Clique em **Avançar** para confirmar a execução da tarefa.

8.5 Restauração do banco de dados

Esta tarefa permitirá que você restaure o banco de dados de um arquivo de backup. As configurações na primeira janela são semelhantes àquelas na conversão do banco de dados (consulte o capítulo Transferência do banco de dados 129); nesta janela, o tipo de banco de dados será selecionado.

Para todos os tipos de banco de dados, além do banco de dados do MS Access, selecione se deseja criar as tabelas de banco de dados automaticamente (**Criar tabelas automaticamente no banco de dados**) ou inserir as tabelas no banco de dados posteriormente (**Visualizar script** > **Salvar em arquivo**) na próxima etapa. Para um banco de dados do MS SQL, a opção **Criar um novo banco de dados ESETRADB automaticamente** criará automaticamente um novo banco de dados do MS SQL nomeado ESETRADB. A etapa final é confirmar a restauração do banco de dados.

Selecione o arquivo do qual o banco de dados será restaurado na próxima etapa. Parâmetros opcionais na parte inferior da janela permitem que você importe um arquivo de um tipo de banco de dados diferente, como selecionado na etapa anterior (**Permitir importação de um tipo diferente de banco de dados**), bem como que você interrompa o ESET Remote Administrator Server durante a restauração de banco de dados (**Interromper servidor durante o processamento da tarefa**). Clique em **Avançar** para confirmar a execução da tarefa.

8.6 Excluir tabelas

Isso exclui as tabelas atuais do banco de dados. Consequentemente, o banco de dados retornará ao estado em que estava imediatamente após a instalação do ERA Server. As configurações na primeira janela são semelhantes àquelas na conversão do banco de dados (consulte o capítulo Transferência do banco de dados 129); nesta janela, o tipo de banco de dados será selecionado. Na próxima etapa, será solicitado que você confirme a ação. Selecione **Sim, eu concordo** e então clique em **Avançar** para confirmar a ação.

OBSERVAÇÃO: Se um banco de dados MS SQL, MySQL ou Oracle for usado, recomendamos que você pare o ERA Server antes de excluir as tabelas.

Se um banco de dados do MS Access for usado, ele será substituído pelo banco de dados vazio padrão.

8.7 Backup de armazenamento

Esta tarefa realizará um backup de armazenamento, que salvará todos os dados da pasta de armazenamento (*C:\ProgramData\ESET\ESET Remote Administrator\Server\storage* por padrão) em um arquivo de despejo externo (*.dmp). Armazenadas nessa pasta estão algumas configurações e logs do servidor importantes. Clique no símbolo de envelope, na parte inferior, para ir até a pasta na qual deseja que seja feito o backup do armazenamento e insira um nome de arquivo. Você também pode escolher se deseja a opção **Substituir se houver**, caso você queira substituir um arquivo .dmp já existente. Recomenda-se que você deixe a opção **Interromper servidor durante o processamento da tarefa** selecionado, pois a tarefa de backup de armazenamento pode causar uma diminuição no desempenho do servidor. Clicar em **Avançar** e em **Iniciar** iniciará a tarefa.

8.8 Restauração de armazenamento

Essa tarefa realizará uma restauração de armazenamento de um arquivo de despejo (*.dmp) salvo anteriormente. Para obter mais informações, consulte a tarefa de backup de armazenamento. Clique no símbolo de envelope, na parte inferior, para ir até a pasta na qual o arquivo de despejo está localizado. Recomenda-se que você deixe a opção **Interromper servidor durante o processamento da tarefa** selecionado, pois a tarefa de restauração de armazenamento pode causar uma diminuição no desempenho do servidor. Clicar em **Avançar** e em **Iniciar** iniciará a tarefa.

8.9 Instalar nova chave de licença

Para inserir uma nova chave de licença a ser usada pelo servidor, insira o local da nova chave de licença.

Substitua a chave de licença existente, se necessário (**Substituir se houver**) e reinicie o servidor, se necessário (**Forçar início de servidor (no caso de não estar em execução)**). Clique em**Avançar** para confirmar e concluir a ação.

8.10 Modificar configuração do servidor

Esta tarefa inicia o Editor de configuração (se instalado). A conclusão da tarefa abrirá a janela do Editor de configuração e permitirá que você edite as configurações avançadas do ERA Server. Essas configurações também estão acessíveis via **Ferramentas** > **Opções do servidor** > **Avançado** > **Editar configurações avançadas**.

OBSERVAÇÃO: para que esse recurso funcione, o ERA Console deve estar instalado. Você também pode salvar configurações do servidor em um arquivo .xml e carregá-lo posteriormente usando a opção **Carregar todas as configurações do arquivo**.

8.11 Interface da linha de comando

O ESET Remote Administrator Maintenance Tool (ERAtool.exe) também pode funcionar como uma ferramenta da linha de comando, integrando-se em scripts. Quando a ferramenta for executada, ela avaliará os parâmetros, executando cada ação na ordem especificada. Se não forem fornecidos argumentos, o assistente interativo será executado.

Os seguintes comandos são compatíveis:

- */startserver* ou */startservice* - inicia o serviço ESET Remote Administrator Server.
- */stopserver* ou */stopservice* - interrompe o serviço ESET Remote Administrator Server.
- */gui* - inicie o assistente interativo depois de concluir todas as tarefas.

Qualquer parâmetro que não inicie com uma barra será interpretado como um nome de arquivo do script de configuração que deve ser executado. Os scripts de configuração são executados salvando configurações no assistente interativo.

OBSERVAÇÃO: o ERAtool.exe exige direitos elevados de administrador; se o script que acionar o ERAtool.exe não tiver os direitos necessários, o Windows poderá exibir um prompt interativo para elevação ou executar a ferramenta em um processo de console separado (perdendo a saída da ferramenta).

9. Solução de problemas

9.1 FAQ

Este capítulo contém soluções para as perguntas mais frequentes e problemas relacionados à instalação e à operação do ERA.

9.1.1 Problemas com a instalação do ESET Remote Administrator no Windows Server 2000/2003

Causa:

uma das possíveis causas pode ser o Terminal Server em execução no sistema no modo *execution*.

Solução:

a Microsoft aconselha alternar do Terminal Server para o modo *"install"* ao instalar programas em um sistema com o serviço Terminal Server em execução. Isso pode ser feito através do **Painel de controle** > **Adicionar/remover programas** ou abrindo um prompt de comando e emitindo o comando *change user /install*. Depois da instalação, digite *change user /execute* para retornar o Terminal Server ao modo de execução. Para obter instruções detalhadas sobre esse processo, consulte o seguinte artigo: http://support.microsoft.com/kb/320185.

9.1.2 Qual é o significado do código de erro GLE?

A instalação do ESET Smart Security ou do ESET NOD32 Antivirus via ESET Remote Administrator Console ocasionalmente pode gerar um erro GLE. Para descobrir o significado de qualquer número de erro GLE, siga estas etapas:

1) Abra um prompt de comando clicando em **Iniciar** > **Executar**. Digite *cmd* e clique em **OK**.
2) No prompt de comando, digite: *net helpmsg error_number*

Exemplo: *net helpmsg* 55

Resultado do exemplo: o recurso ou dispositivo especificado da rede não está mais disponível.

9.2 Códigos de erros frequentemente encontrados

Durante a operação do ERA, você pode receber mensagens de erro, que contêm códigos de erros indicando um problema com algum recurso ou operação. Os capítulos a seguir descrevem os códigos de erros mais frequentemente observados ao realizar instalações forçadas, bem como erros que podem ser encontrados no log do ERAS.

9.2.1 Mensagens de erro exibidas ao usar o ESET Remote Administrator para instalar remotamente o ESET Smart Security ou o ESET NOD32 Antivirus

Código de erro 6 SC, código de erro 53 GLE Não foi possível configurar conexão de IPC para computador de destino
Para configurar uma conexão IPC, estes requisitos devem ser atendidos:

1. Pilha TCP/IP instalada no computador onde o ERAS está instalado, bem como no computador de destino.

2. O compartilhamento de arquivos e impressoras para rede Microsoft deve ser instalado.

3. As portas de compartilhamento de arquivos devem estar abertas (135-139, 445).

4. O computador de destino deve responder a solicitações de ping.

Código de erro 6 SC, código de erro 67 GLE Não foi possível instalar o Instalador da ESET no computador de destino
O compartilhamento administrativo *ADMIN$* deve estar acessível na unidade de sistema do cliente.

Código de erro 6 SC, código de erro 1326 GLE Não foi possível configurar uma conexão de IPC para o computador de destino, provavelmente devido a um nome de usuário ou senha errado
O nome de usuário e senha do administrador não foram digitados corretamente ou não foram inseridos.

Código de erro 6 SC, código de erro 1327 GLE Não foi possível configurar conexão de IPC para computador de destino
O campo de senha do administrador está em branco. Uma instalação forçada remota não pode funcionar com um campo de senha em branco.

Código de erro 11 SC, código de erro 5 GLE Não foi possível instalar o Instalador da ESET no computador de destino
O instalador não pode acessar o computador cliente devido a direitos de acesso insuficientes (acesso negado).

Código de erro 11 SC, código de erro 1726 GLE Não foi possível instalar o Instalador da ESET no computador de destino
Esse código de erro é exibido depois de repetidas tentativas de instalação se a janela de instalação forçada não tiver sido fechada depois da primeira tentativa.

9.2.2 Códigos de erros frequentemente encontrados no era.log

0x1203 - UPD_RETVAL_BAD_URL
Erro do módulo de atualização - nome do servidor de atualização inserido incorretamente.

0x1204 - UPD_RETVAL_CANT_DOWNLOAD
Esse erro pode aparecer:

- ao atualizar através de HTTP
  - o servidor de atualização retorna um código de erro HTTP entre 400 e 500, exceto 401, 403, 404 e 407
  - se as atualizações forem baixadas de um servidor baseado em CISCO e o formato da resposta de autenticação HTTP tiver sido alterado
- ao atualizar de uma pasta compartilhada:
  - o erro retornado não se encaixa nas categorias de autenticação incorreta ou arquivo não encontrado (p. ex., *conexão interrompida* ou *servidor não existente*, etc.)
- ambos os métodos de atualização
  - se todos os servidores relacionados no arquivo *upd.ver* não puderem ser encontrados (o arquivo está localizado em *%ALLUSERSPROFILE%\Application Data\ESET\ESET Remote Administrator\Server\updfiles*)
  - falha ao contatar o servidor protegido contra falhas (provavelmente devido à exclusão das entradas ESET correspondentes no registro)
- configuração do servidor proxy incorreta no ERAS
  - O administrador deve especificar o servidor proxy no formato apropriado.

0x2001 - UPD_RETVAL_AUTHORIZATION_FAILED
Falha na autenticação no servidor de atualização; nome de usuário ou senha incorreta.

0x2102 - UPD_RETVAL_BAD_REPLY
Este erro do módulo de atualização pode ser encontrado se um servidor proxy for usado para mediar a conexão com a Internet - a saber, proxy Webwasher.

0x2104 - UPD_RETVAL_SERVER_ERROR
Erro do módulo de atualizando indicando um código de erro HTTP superior a 500. Se o servidor HTTP da ESET estiver sendo usado, o erro 500 indica um problema com alocação de memória.

0x2105 - UPD_RETVAL_INTERRUPTED
Este erro do módulo de atualização pode ser encontrado se um servidor proxy for usado para mediar a conexão com a Internet - a saber, proxy Webwasher.

9.3 Como diagnosticar problemas com o ERAS?

Se você suspeitar que haja algo errado com o ERAS ou se ele não estiver funcionando corretamente, recomendamos que você siga estas etapas:

1) Verifique o log do ERAS: clique em **Ferramentas** > **Opções do servidor** no menu principal do ERAC. Na janela **Opções do servidor**, clique na guia **Registro em log** e clique em **Exibir log**.

2) Se você não vir mensagens de erro, aumente o nível **Detalhamento de log** na janela **Opções do servidor** para Nível 5. Depois de ter verificado o problema, recomendamos alternar de volta para o valor padrão.

3) Você também pode resolver problemas ativando o log de depuração do banco de dados na mesma guia - consulte a seção **Log de depuração**. Recomendamos que você ative o **Log de depuração** somente ao tentar duplicar o problema.

4) Se você vir quaisquer códigos de erro que não sejam os mencionados nesta documentação, entre em contato com o Atendimento ao cliente da ESET. Descreva o comportamento do programa, como replicar o problema ou como evitá-lo. É muito importante incluir a versão do programa de todos os produtos de segurança da ESET envolvidos (ou seja, ERAS, ERAC, ESET Smart Security, ESET NOD32 Antivirus).

10. Sugestões e dicas

10.1 Agenda

O ESET NOD32 Antivirus e o ESET Smart Security contêm um agenda integrada de tarefas, que permite o agendamento de rastreamentos regulares no computador, atualizações, etc. Todas as tarefas especificadas são relacionadas na Agenda.

Os seguintes tipos de tarefas podem ser configurados usando o ERA:

- Execução de aplicativo externo
- Manutenção de logs
- Rastreamento do computador
- Criação de um instantâneo do status do computador
- Atualização
- Verificação automática de arquivos durante inicialização do sistema

Na maioria dos casos, não há necessidade de configurar uma tarefa **Executar aplicativo externo**. A tarefa **Verificação automática de arquivos durante inicialização do sistema** é uma tarefa padrão e recomendamos não alterar seus parâmetros. Se não forem feitas alterações depois da instalação, o ESET NOD32 e o ESET Smart Security terão duas tarefas predefinidas desse tipo. A primeira tarefa verificará os arquivos do sistema em cada logon do usuário; a segunda tarefa fará o mesmo depois de uma atualização bem-sucedida do banco de dados de assinatura de vírus. De um ponto de vista do administrador, as tarefas **Rastreamento do computador** e **Atualização** são provavelmente as mais úteis:

- **Rastreamento do computador** - essa opção fornece rastreamento regular antivírus (geralmente de unidades locais) em clientes.
- **Atualização** - essa tarefa é responsável por atualizar soluções clientes da ESET. Ela é uma tarefa predefinida e, por padrão, é executada a cada 60 minutos. Geralmente, não há motivo para modificar seus parâmetros. A única exceção é para notebooks, pois seus proprietários frequentemente conectam-se à Internet fora das redes locais. Nesse caso, a tarefa de atualização poderá ser modificada para usar dois perfis de atualização em uma tarefa. Isso permitirá que notebooks sejam atualizados do servidor de imagem local, bem como de servidores de atualização da ESET.

A configuração da Agenda também pode ser encontrada no **Editor de configuração da ESET** em **Linha de produto do Windows v3 e v4** > **Kernel da ESET** > **Configurações** > **Agenda/Planejamento** > **Editar**.

Para obter mais informações, consulte o capítulo Editor de configuração da ESET 50.

A janela da caixa de diálogo pode conter tarefas existentes (clique em **Editar** para modificá-las) ou ela pode estar em branco. Isso depende se você abriu uma configuração de um cliente (p. ex., de um cliente operacional e configurado anteriormente) ou se abriu um novo arquivo com o modelo padrão não contendo tarefas.

Cada nova tarefa recebe uma ID de atributo. As tarefas padrão têm IDs decimais (1, 2, 3...) e as tarefas personalizadas recebem chaves hexadecimais (p. ex., *4AE13D6C*), que são automaticamente geradas ao criar uma nova tarefa.

Se a caixa de seleção de uma tarefa for marcada, isso significa que a tarefa está ativa e que será realizada no cliente especificado.

Os botões na janela Tarefas agendadas funcionam da seguinte forma:

- **Adicionar** - adiciona uma nova tarefa.
- **Editar** - modifica tarefas selecionadas.
- **Alterar ID** - modifica a ID de tarefas selecionadas.
- **Detalhes** - informações de resumo sobre as tarefas selecionadas.
- **Marcar para exclusão** - a aplicação do arquivo *.xml* removerá tarefas (com a mesma ID) selecionadas clicando nesse botão a partir de clientes de destino.
- **Remover da lista** - exclui as tarefas selecionadas da lista. Observe que as tarefas removidas da lista na configuração .xml não serão removidas de estações de trabalho de destino.

Ao criar uma nova tarefa (botão **Adicionar**) ou ao editar uma existente (**Editar**), você deverá especificar quando ela será executada. A tarefa poderá ser repetida depois de determinado período de tempo (a cada dia em 12, a cada sexta-feira, etc.) ou pode ser acionada por um evento (depois de uma atualização bem-sucedida, na primeira vez que o computador iniciar a cada dia, etc.).

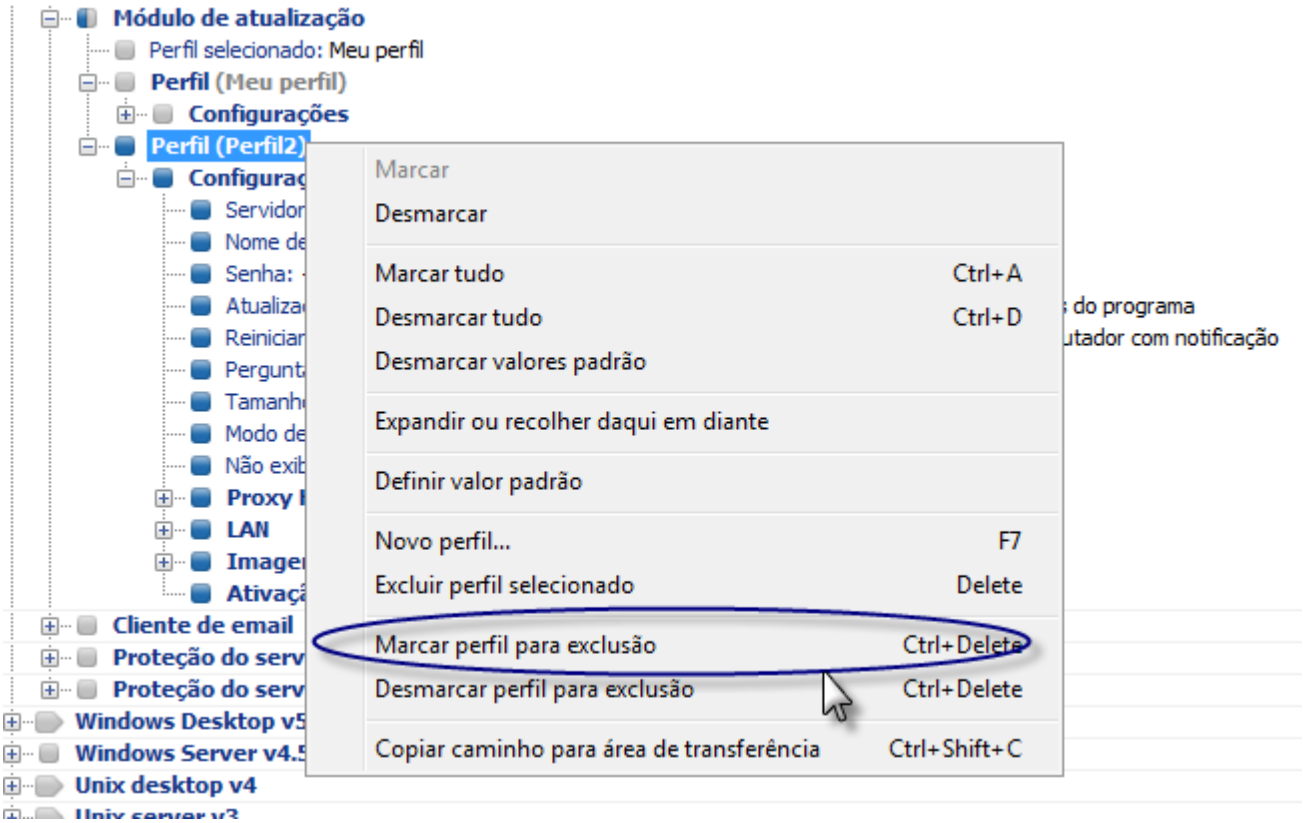
A última etapa da tarefa **Rastreamentos do computador sob demanda** mostra a janela de configurações especiais, na qual você pode definir qual configuração será usada para rastreamento - ou seja, qual perfil de rastreamento e alvos de rastreamento serão usados.

A última etapa da tarefa **Atualização** especifica quais perfis de atualização serão executados na tarefa especificada. Ela é uma tarefa predefinida e, por padrão, é executada a cada 60 minutos. Geralmente, não há motivo para modificar seus parâmetros. A única exceção é para notebooks, pois seus proprietários também se conectam à Internet fora de redes da empresa. A última caixa de diálogo permite que você especifique dois perfis de atualização diferentes, cobrindo atualizações de um servidor local ou de servidores de atualização da ESET.

10.2 Removendo perfis existentes

Ocasionalmente, você pode se deparar com perfis duplicados (perfis de atualização ou rastreamento) que foram criados por engano. Para remover esses perfis remotamente sem causar danos a outras configurações na Agenda, siga estas etapas:

- No ERAC, clique na guia **Clientes** e dê um duplo clique em um cliente problemático.
- Na janela **Propriedades do cliente**, clique na guia **Configuração**. Selecione as opções **Em seguida, execute o Editor de configuração da ESET para editar o arquivo** e **Use a configuração baixada na nova tarefa de configuração**; em seguida, clique no botão **Nova tarefa**.
- No assistente de nova tarefa, clique em **Editar**.
- No Editor de configuração, pressione **CTRL + D** para desmarcar (esmaecer) todas as configurações). Isso ajuda a impedir alterações acidentais, pois quaisquer novas alterações ficarão em azul.
- Clique com o botão direito do mouse no perfil que você deseja remover e selecione **Marcar perfil para exclusão** no menu de contexto. O perfil será excluído assim que a tarefa for entregue aos clientes.



- Clique no botão **Console** no Editor de configuração da ESET e salve as configurações.
- Verifique se o cliente selecionado está na coluna **Itens selecionados** à direita. Clique em **Avançar** e, em seguida, clique em **Concluir**.

10.3 Exportação e outros recursos da configuração XML do cliente

No ERAC, selecione quaisquer clientes na guia **Clientes**. Clique com o botão direito do mouse e selecione **Configuração...** no menu de contexto. Clique em **Salvar como...** para exportar a configuração atribuída do cliente especificado para um arquivo *.xml* (os arquivos de configuração *.xml* também podem ser extraídos diretamente da interface do programa ESET Smart Security). O arquivo *.xml* pode ser usado posteriormente para várias operações:

- Para instalações remotas, o arquivo *.xml* pode ser usado como um modelo para uma configuração predefinida. Isso significa que nenhum novo arquivo *.xml* foi criado e que o arquivo *.xml* existente foi atribuído (**Selecionar...**) a um novo pacote de instalação. Os arquivos de configuração *.xml* também podem ser extraídos diretamente da interface do programa ESET Smart Security.
- Para configurar vários clientes, os clientes selecionados recebem um arquivo *.xml* baixado anteriormente e adotam as configurações que estão definidas no arquivo (nenhuma nova configuração é criada, somente atribuída pelo botão **Selecionar...**).

Exemplo

Um produto de segurança da ESET está instalado somente em uma estação de trabalho. Ajuste as configurações diretamente através da interface do usuário do programa. Quando tiver concluído, exporte as configurações para um arquivo *.xml*. Esse arquivo *.xml* poderá então ser usado para instalações remotas em outras estações de trabalho. Esse método pode ser muito útil para tarefas como ajuste de regras de firewall se o modo *"com base em políticas"* precisar ser aplicado.

10.4 Atualização combinada para notebooks

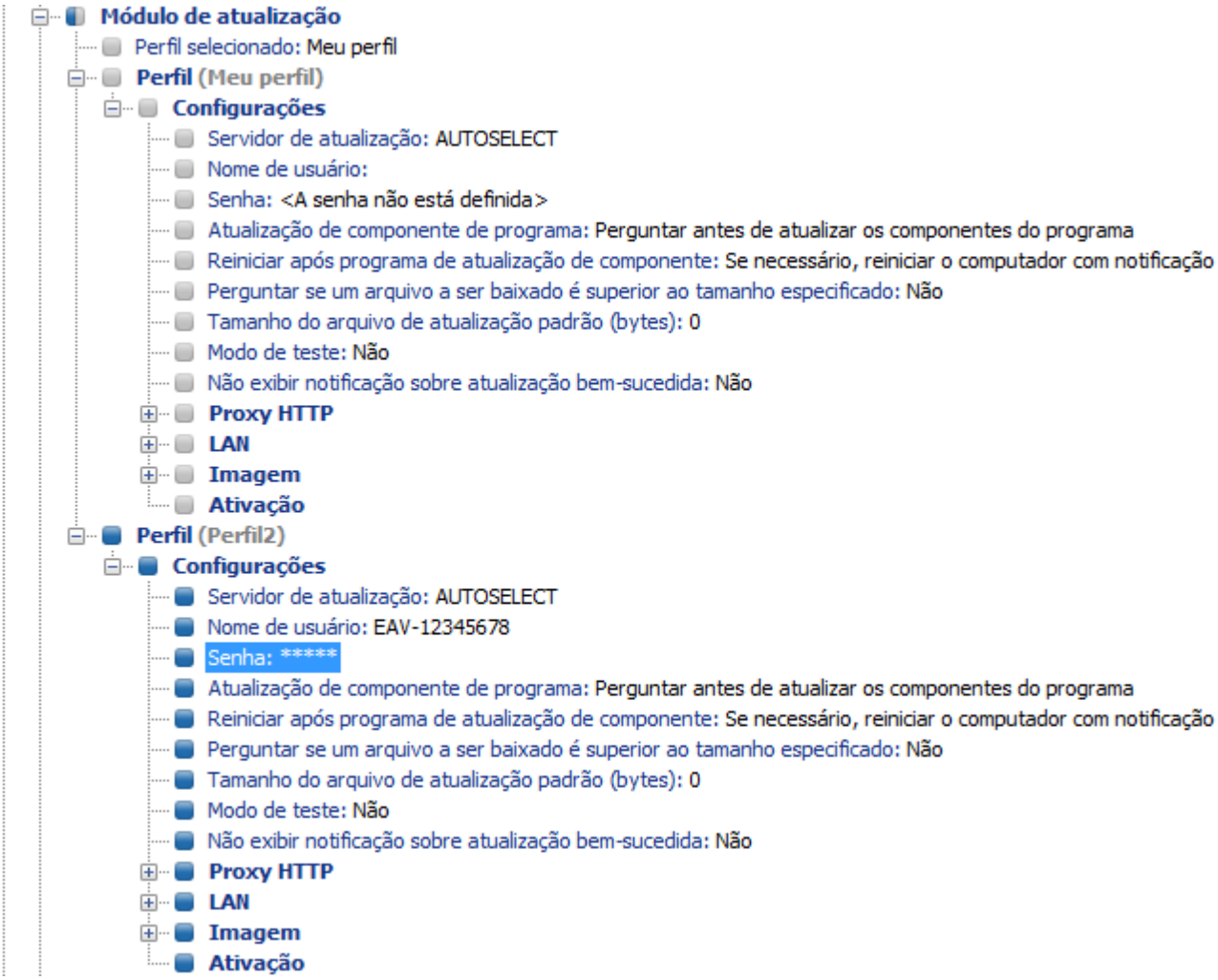
Se houver dispositivos móveis em sua rede local (ou seja, notebooks), recomendamos que você configure uma atualização combinada de duas fontes: servidores de atualização da ESET e o servidor de Imagem local. Primeiro, os notebooks contatam o servidor de Imagem local e, se a conexão falhar (eles estão fora do escritório), eles farão download de atualizações diretamente de servidores da ESET. Para permitir essa funcionalidade:

- Crie dois perfis de atualização, Exportação e outros recursos da configuração XML do cliente 137 um direcionado para o servidor de Imagem (referido como "LAN" no exemplo a seguir) e o segundo para os servidores de atualização da ESET (INET)
- Crie uma nova tarefa de atualização ou modifique uma tarefa de atualização existente através da Agenda (**Ferramentas** > **Agenda** da janela principal do programa do ESET Smart Security ou ESET NOD32 Antivirus).

A configuração pode ser feita diretamente em notebooks ou remotamente usando o Editor de configuração da ESET. Ela também pode ser aplicada durante a instalação ou a qualquer momento posteriormente como uma tarefa de configuração.

Para criar novos perfis no Editor de configuração da ESET, clique com o botão direito do mouse na ramificação **Atualizar** e selecione **Novo perfil** no menu de contexto.

O resultado de modificações deve ser semelhante ao exibido a seguir:


Módulo de atualização
Perfil selecionado: Meu perfil
Perfil (Meu perfil)
Configurações
Servidor de atualização: AUTOSELECT
Nome de usuário:
Senha: <A senha não está definida>
Atualização de componente de programa: Perguntar antes de atualizar os componentes do programa
Reiniciar após programa de atualização de componente: Se necessário, reiniciar o computador com notificação
Perguntar se um arquivo a ser baixado é superior ao tamanho especificado: Não
Tamanho do arquivo de atualização padrão (bytes): 0
Modo de teste: Não
Não exibir notificação sobre atualização bem-sucedida: Não
Proxy HTTP
LAN
Imagem
Ativação
Perfil (Perfil2)
Configurações
Servidor de atualização: AUTOSELECT
Nome de usuário: EAV-12345678
Senha: *****
Atualização de componente de programa: Perguntar antes de atualizar os componentes do programa
Reiniciar após programa de atualização de componente: Se necessário, reiniciar o computador com notificação
Perguntar se um arquivo a ser baixado é superior ao tamanho especificado: Não
Tamanho do arquivo de atualização padrão (bytes): 0
Modo de teste: Não
Não exibir notificação sobre atualização bem-sucedida: Não
Proxy HTTP
LAN
Imagem
Ativação

A LAN do perfil fará download de atualizações do servidor de Imagem local da empresa (*http://server:2221*), enquanto o INET do perfil se conecta a servidores da ESET (**Escolher automaticamente**). Em seguida, defina uma tarefa de atualização executada em cada perfil de atualização em sucessão. Para fazer isso, acesse **Linha de produto do Windows v3 e v4** > **Kernel da ESET** > **Configurações** > **Agenda/Planejamento** no Editor de configuração da ESET. Clique no botão **Editar** para exibir a janela **Tarefas agendadas**.

Para criar uma nova tarefa, clique em **Adicionar**. No menu suspenso **Tarefa agendada**, selecione **Atualizar** e clique em **Avançar**. Insira o **Nome da tarefa** (p. ex., *"atualização combinada"*), selecione **Repetidamente a cada 60 minutos** e prossiga para a seleção de um perfil primário e secundário.

Se as estações de trabalho de notebook devem contatar o servidor de Imagem primeiro, o perfil Primário deverá ser definido como LAN e o secundário como INET. O INET do perfil seria aplicado somente se a atualização da LAN falhar.

Recomendação: exporte a configuração *.xml* atual de um cliente (para obter mais informações, consulte o capítulo Como diagnosticar problemas com o ERAS? 133) e realize as modificações mencionadas acima no arquivo *.xml* exportado. Isso impedirá qualquer duplicação entre a Agenda e perfis não operacionais.

10.5 Instalação de produtos de terceiros usando o ERA

Além da instalação remota de produtos da ESET, o ESET Remote Administrator é capaz de instalar outros programas. O único requisito é que o pacote de instalação personalizada deve estar no formato *.msi*. A instalação remota dos pacotes personalizados pode ser realizada usando um processo muito semelhante ao descrito no capítulo Instalação forçada remota 55.

A principal diferença está no processo de criação do pacote, que é o seguinte:

1) No ERAC, clique na guia **Instalação remota**.

2) Selecione a guia **Computadores** e clique com o botão direito do mouse em qualquer parte em seu conteúdo. Selecione **Gerenciar pacotes** no menu de contexto.

3) No menu suspenso Tipo de pacote, selecione **Pacote personalizado**.

4) Clique em **Adicionar...**, clique em **Adicionar arquivo** e selecione o pacote *.msi* desejado.

5) Selecione o arquivo no menu suspenso **Arquivo de entrada de pacote** e clique em **Criar**.

6) Depois de retornar para a janela original, você poderá especificar parâmetros da linha de comando para o arquivo *.msi*. Os parâmetros são os mesmos para uma instalação local do pacote especificado.

7) Clique em **Salvar como...** para salvar o pacote.

8) Clique em **Fechar** para sair do editor do pacote de instalação.

O pacote personalizado recém-criado poderá ser distribuído para estações de trabalho clientes da mesma forma que as instalações remotas descritas em capítulos anteriores. Uma instalação forçada remota, instalação forçada por logon ou e-mail enviará o pacote para estações de trabalho de destino. Quando o pacote é aberto, a instalação é processada pelo serviço Microsoft Windows Installer. Depois de completar a instalação personalizada, o ERAS pode fazer download de um arquivo do cliente que contem os dados do resultado de instalação. Para especificar um arquivo de resultado, adicione o parâmetro **/eResult** na linha de comando associada com o pacote depois de salvar o pacote personalizado. Depois de executar a tarefa de instalação personalizada, faça o download dos arquivos de resultado do ERAS na janela **Detalhes de tarefa**.

OBSERVAÇÃO: Existe um limite de tamanho de 100 mb para pacotes de instalação personalizados de terceiros.

11. ESET SysInspector

11.1 Introdução ao ESET SysInspector

O ESET SysInspector é um aplicativo que inspeciona completamente o seu computador e exibe os dados coletados de uma maneira abrangente. Informações como drivers e aplicativos instalados, conexões de rede ou entradas importantes de registro podem ajudá-lo a investigar o comportamento suspeito do sistema, seja devido a incompatibilidade de software ou hardware ou infecção por malware.

É possível acessar o ESET SysInspector de duas formas: Na versão integrada nas soluções ESET Security ou por meio de download da versão autônoma (SysInspector.exe) gratuita no site da ESET. Ambas as versões têm funções idênticas e os mesmos controles de programa. A única diferença é a forma como os resultados são gerenciados. As versões integrada e autônoma permitem exportar instantâneos do sistema em um arquivo *.xml* e salvá-los em disco. Entretanto, a versão integrada também permite armazenar os instantâneos do sistema diretamente em**Ferramentas** > **ESET SysInspector** (exceto ESET Remote Administrator).

Aguarde enquanto o ESET SysInspector rastreia o computador. Pode demorar de 10 segundos a alguns minutos, dependendo da configuração de hardware, do sistema operacional e da quantidade de aplicativos instalados no computador.

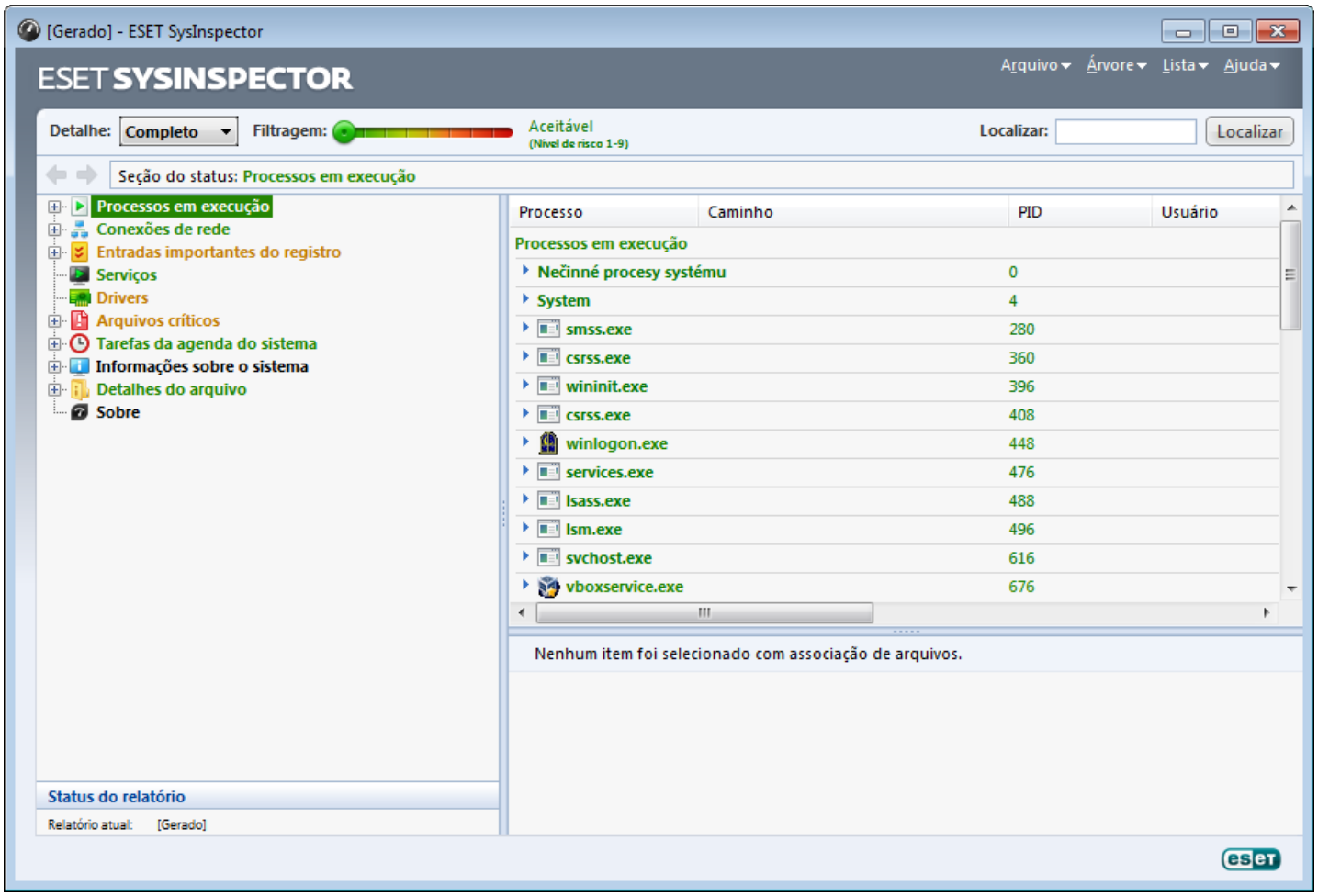
11.1.1 Iniciando ESET SysInspector

Para iniciar o ESET SysInspector, basta executar o arquivo executável *SysInspector.exe* obtido por download no site da ESET.

Aguarde enquanto o aplicativo inspeciona o sistema, o que pode demorar vários minutos, dependendo do hardware e dos dados a serem coletados.

11.2 Interface do usuário e uso do aplicativo

Para maior clareza, a janela principal é dividida em quatro seções principais - Controles do programa localizados na parte superior da janela principal, a janela Navegação à esquerda, a janela Descrição à direita, no meio, e a janela Detalhes à direita, na parte inferior da janela principal. A seção Status do log lista os parâmetros básicos de um log (filtro usado, tipo de filtro, se o log é o resultado de uma comparação, etc.).



11.2.1 Controles do programa

Esta seção contém a descrição de todos os controles do programa disponíveis no ESET SysInspector.

Arquivo

Clicando em **Arquivo**, você pode armazenar o status atual do sistema para investigação posterior ou abrir um log armazenado anteriormente. Por motivo de publicação, recomendamos a geração de um log **Adequado para envio**. Neste formulário, o log omite informações confidenciais (nome do usuário atual, nome do computador, nome do domínio, privilégios do usuário atual, variáveis do ambiente, etc.).

OBSERVAÇÃO: Você pode abrir os relatórios do ESET SysInspector armazenados anteriormente simplesmente arrastando e soltando-os na janela principal.

Árvore

Permite expandir ou fechar todos os nós e exportar as seções selecionadas para o script de serviços.

Lista

Contém funções para uma navegação mais fácil dentro do programa e diversas outras funções, como, por exemplo, encontrar informações online.

Ajuda

Contém informações sobre o aplicativo e as funções dele.

Detalhe

Esta configuração influencia as informações exibidas na janela principal para facilitar o trabalho com as informações. No modo "Básico", você terá acesso a informações utilizadas para encontrar soluções para problemas comuns no seu sistema. No modo "Médio", o programa exibe detalhes menos usados. No modo "Completo", o ESET SysInspector exibe todas as informações necessárias para resolver problemas muito específicos.

Filtragem de itens

A filtragem de itens é mais adequada para encontrar arquivos suspeitos ou entradas do registro no sistema. Ajustando o controle deslizante, você pode filtrar itens pelo nível de risco deles. Se o controle deslizante estiver configurado todo para a esquerda (Nível de risco 1), todos os itens serão exibidos. Se você mover o controle deslizante para a direita, o programa filtrará todos os itens menos perigosos que o nível de risco atual e exibirá apenas os itens que são mais suspeitos que o nível exibido. Com o controle deslizante todo para a direita, o programa exibirá apenas os itens perigosos conhecidos.

Todos os itens identificados como de risco 6 a 9 podem colocar a segurança em risco. Se você não estiver utilizando uma solução de segurança da ESET, recomendamos que você rastreie o sistema com o ESET Online Scanner se o ESET SysInspector encontrou esse item. O ESET Online Scanner é um serviço gratuito.

OBSERVAÇÃO: O nível de risco de um item pode ser rapidamente determinado comparando a cor do item com a cor no controle deslizante Nível de risco.

Procurar

A opção Pesquisar pode ser utilizada para encontrar um item específico pelo nome ou por parte do nome. Os resultados da solicitação da pesquisa são exibidos na janela Descrição.

Retornar

Clicando na seta para trás e para a frente, você pode retornar para as informações exibidas anteriormente na janela Descrição. Você pode usar as teclas Backspace e de espaço em vez de clicar para trás e para a frente.

Seção do status

Exibe o nó atual na janela Navegação.

Importante: Os itens realçados em vermelho são desconhecidos, por isso o programa os marca como potencialmente perigosos. Se um item estiver em vermelho, isso não significa automaticamente que você pode excluir o arquivo. Antes de excluir, certifique-se de que os arquivos são realmente perigosos ou desnecessários.

11.2.2 Navegação no ESET SysInspector

O ESET SysInspector divide vários tipos de informações em diversas seções básicas chamadas de nós. Se disponíveis, você pode encontrar detalhes adicionais expandindo cada nó em seus subnós. Para abrir ou recolher um nó, clique duas vezes no nome do nó ou, como alternativa, clique em ⊞ ou ⊟ próximo ao nome do nó. À medida que percorrer a estrutura em árvore dos nós e subnós na janela Navegação, você pode encontrar diversos detalhes para cada nó mostrado na janela Descrição. Se você percorrer os itens na janela Descrição, detalhes adicionais sobre cada item podem ser exibidos na janela Detalhes.

A seguir estão as descrições dos nós principais na janela Navegação e as informações relacionadas nas janelas Descrição e Detalhes.

Processos em execução

Esse nó contém informações sobre aplicativos e processos em execução no momento da geração do log. Na janela Descrição, você pode encontrar detalhes adicionais para cada processo, como, por exemplo, bibliotecas dinâmicas usadas pelo processo e o local delas no sistema, o nome do fornecedor do aplicativo, o nível de risco do arquivo, etc.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

OBSERVAÇÃO: Um sistema operacional consiste em diversos componentes kernel importantes que são executados 24 horas por dia, 7 dias por semana e que fornecem funções básicas e vitais para outros aplicativos de usuários. Em determinados casos, tais processos são exibidos na ferramenta ESET SysInspector com o caminho do arquivo começando com \??\. Esses símbolos fornecem otimização de pré-início para esses processos; eles são seguros para o sistema.

Conexões de rede

A janela Descrição contém uma lista de processos e aplicativos que se comunicam pela rede utilizando o protocolo selecionado na janela Navegação (TCP ou UDP), junto com os endereços remotos aos quais o aplicativo está conectado. Também é possível verificar os endereços IP dos servidores DNS.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

Entradas importantes do registro

Contém uma lista de entradas de registro selecionadas que estão relacionadas frequentemente a diversos problemas com o sistema, como aqueles que especificam os programas de inicialização, objetos auxiliares do navegador (BHO), etc.

Na janela Descrição, é possível localizar quais arquivos estão relacionados a entradas de registro específicas. Você pode consultar detalhes adicionais na janela Detalhes.

Serviços

A janela Descrição contém uma lista de arquivos registrados como serviços do Windows. É possível verificar a maneira como o serviço é configurado para iniciar, junto com detalhes específicos do arquivo na janela Detalhes.

Drivers

Uma lista de drivers instalados no sistema.

Arquivos críticos

A janela Descrição exibe o conteúdo dos arquivos críticos relacionados ao sistema operacional Microsoft Windows.

Tarefas da agenda do sistema

Contém uma lista de tarefas acionadas pela Agenda de Tarefas do Windows em uma hora/intervalo específico.

Informações sobre o sistema

Contém informações detalhadas sobre hardware e software, além de informações sobre as variáveis ambientais configuradas, os direitos do usuário e os registros de eventos do sistema.

Detalhes do arquivo

Uma lista de arquivos importantes do sistema e arquivos na pasta Arquivos de programas. Informações adicionais específicas dos arquivos podem ser encontradas nas janelas Descrição e Detalhes.

Sobre

Informações sobre a versão do ESET SysInspector e a lista dos módulos do programa.

11.2.2.1 Atalhos do teclado

Teclas de atalho que podem ser usadas ao trabalhar com o ESET SysInspector incluem:

Arquivo

Ctrl+O	Abre o log existente
Ctrl+S	Salva os logs criados

Gerar

Ctrl+G	gera um instantâneo padrão do status do computador
Ctrl+H	gera um instantâneo do status do computador que também pode registrar informações confidenciais

Filtragem de itens

1, O	Aceitável, nível de risco 1-9, os itens são exibidos
2	Aceitável, nível de risco 2-9, os itens são exibidos
3	Aceitável, nível de risco 3-9, os itens são exibidos
4, U	Desconhecido, nível de risco 4-9, os itens são exibidos
5	Desconhecido, nível de risco 5-9, os itens são exibidos
6	Desconhecido, nível de risco 6-9, os itens são exibidos

7, B	Perigoso, nível de risco 7-9, os itens são exibidos
8	Perigoso, nível de risco 8-9, os itens são exibidos
9	Perigoso, nível de risco 9, os itens são exibidos
-	Diminui o nível de risco
+	Aumenta o nível de risco
Ctrl+9	Modo de filtragem, nível igual ou superior
Ctrl+O	Modo de filtragem, somente nível igual

Visualizar

Ctrl+5	Exibição por fornecedor, todos os fornecedores
Ctrl+6	Exibição por fornecedor, somente Microsoft
Ctrl+7	Exibição por fornecedor, todos os outros fornecedores
Ctrl+3	Exibe detalhes completos
Ctrl+2	Exibe detalhes da mídia
Ctrl+1	Exibição básica
Backspace	Move um passo para trás
Espaço	Move um passo para a frente
Ctrl+W	Expande a árvore
Ctrl+Q	Recolhe a árvore

Outros controles

Ctrl+T	Vai para o local original do item após a seleção nos resultados de pesquisa
Ctrl+P	Exibe informações básicas sobre um item
Ctrl+A	Exibe informações completas sobre um item
Ctrl+C	Copia a árvore do item atual
Ctrl+X	Copia itens
Ctrl+B	Localiza informações sobre os arquivos selecionados na Internet
Ctrl+L	Abre a pasta em que o arquivo selecionado está localizado
Ctrl+R	Abre a entrada correspondente no editor do registro
Ctrl+Z	Copia um caminho para um arquivo (se o item estiver relacionado a um arquivo)
Ctrl+F	Alterna para o campo de pesquisa
Ctrl+D	Fecha os resultados da pesquisa
Ctrl+E	Executa script de serviços

Comparação

Ctrl+Alt+O	Abre o log original/comparativo
Ctrl+Alt+R	Cancela a comparação
Ctrl+Alt+1	Exibe todos os itens
Ctrl+Alt+2	Exibe apenas os itens adicionados; o log mostrará os itens presentes no log atual
Ctrl+Alt+3	Exibe apenas os itens removidos; o log mostrará os itens presentes no log anterior
Ctrl+Alt+4	Exibe apenas os itens substituídos (arquivos inclusive)
Ctrl+Alt+5	Exibe apenas as diferenças entre os logs
Ctrl+Alt+C	Exibe a comparação
Ctrl+Alt+N	Exibe o log atual
Ctrl+Alt+P	Exibe o log anterior

Diversos

F1	Exibe a Ajuda
Alt+F4	Fecha o programa
Alt+Shift+F4	Fecha o programa sem perguntar
Ctrl+I	Estatísticas de logs

11.2.3 Comparar

O recurso Comparar permite que o usuário compare dois logs existentes. O resultado desse recurso é um conjunto de itens não comuns em ambos os logs. Ele é adequado se você desejar manter controle das alterações no sistema, uma ferramenta útil para detectar atividade de código malicioso.

Após ser iniciado, o aplicativo criará um novo log, que será exibido em uma nova janela. Navegue até **Arquivo** > **Salvar relatório** para salvar um log em um arquivo. Os arquivos de log podem ser abertos e visualizados posteriormente. Para abrir um log existente, utilize **Arquivo** > **Abrir relatório**. Na janela principal do programa, o ESET SysInspector sempre exibe um log de cada vez.

O benefício de comparar dois logs é que você pode visualizar um log ativo atual e um log salvo em um arquivo. Para comparar relatórios, use a opção **Arquivo** > **Comparar relatório** e escolha **Selecionar arquivo**. O log selecionado será comparado com o log ativo na janela principal do programa. O log comparativo exibirá somente as diferenças entre esses dois logs.

OBSERVAÇÃO: Caso compare dois arquivos de log, selecione **Arquivo** > **Salvar relatório** para salvá-lo como um arquivo ZIP; ambos os arquivos serão salvos. Se você abrir esse arquivo posteriormente, os logs contidos serão comparados automaticamente.

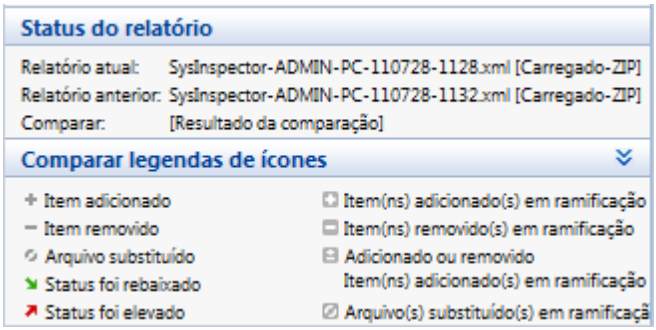
Próximo aos itens exibidos, o ESET SysInspector mostra símbolos que identificam diferenças entre os logs comparados.

Os itens marcados por um – apenas podem ser encontrados no log ativo e não estavam presentes no log comparativo aberto. Os itens marcados por um + estavam presentes apenas no log aberto e estavam ausentes no log ativo.

Descrição de todos os símbolos que podem ser exibidos próximos aos itens:

- + novo valor, não presente no log anterior
- a seção de estrutura em árvore contém novos valores
- – valor removido, presente apenas no log anterior
- a seção de estrutura em árvore contém valores removidos
- o valor/arquivo foi alterado
- a seção de estrutura em árvore contém valores/arquivos modificados
- o nível de risco reduziu / era maior no log anterior
- o nível de risco aumentou / era menor no log anterior

A seção de explicação exibida no canto inferior esquerdo descreve todos os símbolos e também exibe os nomes dos logs que estão sendo comparados.



Qualquer log comparativo pode ser salvo em um arquivo e aberto posteriormente.

Exemplo

Gere e salve um relatório, registrando informações originais sobre o sistema, em um arquivo chamado previous.xml. Após terem sido feitas as alterações, abra o ESET SysInspector e deixe-o gerar um novo relatório. Salve-o em um arquivo chamado *current.xml*.

Para controlar as alterações entre esses dois logs, navegue até **Arquivo** > **Comparar relatórios**. O programa criará um log comparativo mostrando as diferenças entre os logs.

O mesmo resultado poderá ser alcançado se você utilizar a seguinte opção da linha de comandos:

SysIsnpector.exe current.xml previous.xml

11.3 Parâmetros da linha de comando

O ESET SysInspector suporta a geração de relatórios a partir da linha de comando utilizando estes parâmetros:

/gen	gerar um log diretamente a partir da linha de comando sem executar a GUI
/privacy	gerar um log excluindo informações confidenciais
/zip	armazenar o log resultante diretamente no disco em um arquivo compactado
/silent	ocultar a exibição da barra de progresso da geração de logs
/help, /?	exibir informações sobre os parâmetros da linha de comando

Exemplos

Para carregar um log específico diretamente no navegador, use: *SysInspector.exe "c:\clientlog.xml"*
Para gerar um log em um local atual, use: *SysInspector.exe /gen*
Para gerar um log em uma pasta específica, use: *SysInspector.exe /gen="c:\folder\"*
Para gerar um log em um arquivo/local específico, use: *SysInspector.exe /gen="c:\folder\mynewlog.xml"*
Para gerar um log que exclua informações confidenciais diretamente em um arquivo compactado, use: *SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip*
Para comparar dois logs, use: *SysInspector.exe "current.xml" "original.xml"*

OBSERVAÇÃO: Se o nome do arquivo/pasta contiver uma lacuna, ele deve ser colocado entre aspas.

11.4 Script de serviços

O script de serviços é uma ferramenta que fornece ajuda aos clientes que utilizam o ESET SysInspector removendo facilmente os objetos indesejados do sistema.

O script de serviços permite que o usuário exporte o relatório completo do ESET SysInspector ou suas partes selecionadas. Após a exportação, você pode marcar os objetos não desejados para exclusão. Em seguida, você pode executar o log modificado para excluir os objetos marcados.

O script de serviços é adequado para usuários avançados com experiência anterior em diagnóstico de problemas do sistema. As modificações não qualificadas podem levar a danos no sistema operacional.

Exemplo

Se você suspeita que o seu computador está infectado por um vírus que não é detectado pelo seu programa antivírus, siga estas instruções passo a passo:

- Execute o ESET SysInspector para gerar um novo instantâneo do sistema.
- Selecione o primeiro item na seção à esquerda (na estrutura em árvore), pressione Shift e selecione o último item para marcar todos os itens.
- Clique com o botão direito do mouse nos objetos selecionados e selecione a opção do menu de contexto **Exportar as seções selecionadas para script de serviços**.
- Os objetos selecionados serão exportados para um novo log.
- Esta é a etapa mais crucial de todo o procedimento: abra o novo log e altere o atributo - para + em todos os objetos que desejar remover. Verifique se não marcou arquivos/objetos do sistema operacional importantes.
- Abra o ESET SysInspector, clique em **Arquivo** > **Executar script de serviço** e digite o caminho para o script.
- Clique em **OK** para executar o script.

11.4.1 Geração do script de serviços

Para gerar um script, clique com o botão direito em um item na árvore de menus (no painel esquerdo) na janela principal do ESET SysInspector. No menu de contexto, selecione a opção **Exportar todas as seções para script de serviços** ou a opção **Exportar as seções selecionadas para script de serviços**.

OBSERVAÇÃO: Não é possível exportar o script de serviços quando dois logs estiverem sendo comparados.

11.4.2 Estrutura do script de serviços

Na primeira linha do cabeçalho do script, você pode encontrar informações sobre a versão do Mecanismo (ev), versão da GUI (gv) e a versão do log (lv). É possível usar esses dados para rastrear possíveis alterações no arquivo .xml que gera o script e evitar inconsistências durante a execução. Esta parte do script não deve ser alterada.

O restante do arquivo é dividido em seções nas quais os itens podem ser editados (refere-se àqueles que serão processadas pelo script). Marque os itens para processamento substituindo o caractere "-" em frente a um item pelo caractere "+". As seções no script são separadas das outras por uma linha vazia. Cada seção tem um número e um título.

01) Processos em execução

Esta seção contém uma lista de todos os processos em execução no sistema. Cada processo é identificado por seu caminho UNC e, subsequentemente, por seu código hash CRC16 em asteriscos (*).

Exemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Neste exemplo, o processo, module32.exe, foi selecionado (marcado por um caractere "+"); o processo será encerrado com a execução do script.

02) Módulos carregados

Essa seção lista os módulos do sistema em uso no momento.

Exemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Neste exemplo, o módulo khbekhb.dll foi marcado por um caractere "+". Quando o script for executado, ele reconhecerá os processos que usam esse módulo específico e os encerrará.

03) Conexões TCP

Esta seção contém informações sobre as conexões TCP existentes.

Exemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Quando o script for executado, ele localizará o proprietário do soquete nas conexões TCP marcadas e interromperá o soquete, liberando recursos do sistema.

04) Pontos de extremidade UDP

Esta seção contém informações sobre os pontos de extremidade UDP existentes.

Exemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Quando o script for executado, ele isolará o proprietário do soquete nos pontos de extremidade UDP marcados e interromperá o soquete.

05) Entradas do servidor DNS

Esta seção contém informações sobre a configuração atual do servidor DNS.

Exemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

As entradas marcadas do servidor DNS serão removidas quando você executar o script.

06) Entradas importantes do registro

Esta seção contém informações sobre as entradas importantes do registro.

Exemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

As entradas marcadas serão excluídas, reduzidas ao valor de 0 byte ou redefinidas aos valores padrão com a execução do script. A ação a ser aplicada a uma entrada específica depende da categoria da entrada e do valor da chave no registro específico.

07) Serviços

Esta seção lista os serviços registrados no sistema.

Exemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Os serviços marcados e seus serviços dependentes serão interrompidos e desinstalados quando o script for executado.

08) Drivers

Esta seção lista os drivers instalados.

Exemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Ao executar o script, os drivers selecionados serão parados. Observe que alguns drivers não permitirão que sejam parados.

09) Arquivos críticos

Esta seção contém informações sobre os arquivos que são críticos para o funcionamento correto do sistema operacional.

Exemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Os itens selecionados serão excluídos ou redefinidos aos valores padrão originais.

11.4.3 Execução de scripts de serviços

Marque todos os itens desejados, depois salve e feche o script. Execute o script editado diretamente na janela principal do ESET SysInspector selecionando a opção **Executar script de serviços** no menu Arquivo. Ao abrir um script, o programa solicitará que você responda à seguinte email: **Tem certeza de que deseja executar o script de serviços "% Scriptname%"?** Após confirmar a seleção, outro aviso pode ser exibido, informando que o script de serviços que você está tentando executar não foi assinado. Clique em **Executar** para iniciar o script.

Uma janela de diálogo confirmará que o script foi executado com êxito.

Se o script puder ser apenas parcialmente processado, uma janela de diálogo com a seguinte email será exibida: **O script de serviços foi executado parcialmente. Deseja exibir o relatório de erros?** Selecione **Sim** para exibir um relatório de erro complexo que lista as operações que não foram executadas.

Se o script não for reconhecido, uma janela de diálogo com a seguinte email será exibida: **O script de serviços selecionado não está assinado. A execução de scripts não assinados e desconhecidos pode danificar seriamente os dados do computador. Tem certeza de que deseja executar o script e realizar as ações?** Isso pode ser causado por inconsistências no script (cabeçalho danificado, título da seção corrompido, ausência de linha vazia entre as seções, etc.). É possível reabrir o arquivo de script e corrigir os erros no script ou criar um novo script de serviços.

11.5 FAQ

O ESET SysInspector requer privilégios de administrador para ser executado?

Enquanto o ESET SysInspector não requer privilégios de administrador para ser executado, algumas das informações que ele coleta apenas podem ser acessadas a partir de uma conta do administrador. A execução desse programa como Usuário padrão ou Usuário restrito fará com que ele colete menos informações sobre o seu ambiente operacional.

O ESET SysInspector cria um arquivo de log?

o ESET SysInspector pode criar um arquivo de log da configuração do computador. Para salvar um arquivo de log, selecione **Arquivo** > **Salvar relatório** no menu principal. Os arquivos de log são salvos em formato XML. Por padrão, os arquivos são salvos no diretório *%USERPROFILE%\Meus Documentos*\, com a convenção de nomenclatura de arquivos de "SysInpsector-%NOMECOMPUTADOR%-AAMMDD-HHMM.XML". Você pode alterar o local e o nome do arquivo de log para outro nome ou local antes de salvá-lo, se preferir.

Como visualizar o arquivo de log do ESET SysInspector?

Para visualizar um arquivo de log criado pelo ESET SysInspector, execute o programa e selecione **Arquivo** > **Abrir relatório** no menu principal. Você também pode arrastar e soltar arquivos de log no aplicativo ESET SysInspector. Se você precisar visualizar os arquivos de log do ESET SysInspector com frequência, recomendamos a criação de um atalho para o arquivo SYSINSPECTOR.EXE na área de trabalho; é possível arrastar e soltar os arquivos de log para visualização. Por motivo de segurança, o Windows Vista/7 pode não permitir operações de arrastar e soltar entre janelas que tenham permissões de segurança diferentes.

Há uma especificação disponível para o formato do arquivo de log? E um SDK?

Atualmente, não há uma especificação para o arquivo de log nem um SDK disponíveis, uma vez que o programa ainda está em desenvolvimento. Após o lançamento do programa, podemos fornecê-los com base nas informações fornecidas pelos clientes e sob demanda.

Como o ESET SysInspector avalia o risco representado por um objeto específico?

Na maioria dos casos, o ESET SysInspector atribui níveis de risco a objetos (arquivos, processos, chaves de registro e assim por diante), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de risco aos objetos, que vai de 1 - Aceitável (verde) a 9 - Perigoso (vermelho). No painel de navegação esquerdo, as seções são coloridas com base no nível de risco mais alto de um objeto dentro delas.

Um nível de risco "6 - Desconhecido (vermelho)" significa que um objeto é perigoso?

As avaliações do ESET SysInspector não garantem que um objeto seja malicioso; essa determinação deve ser feita por um especialista em segurança. O ESET SysInspector é destinado a fornecer uma avaliação rápida para especialistas em segurança, para que eles saibam quais objetos em um sistema eles poderão querer examinar quanto a comportamento incomum.

Por que o ESET SysInspector conecta-se à Internet quando está em execução?

Como muitos aplicativos, o ESET SysInspector é assinado com um "certificado" de assinatura digital para ajudar a garantir que o software foi publicado pela ESET e que não foi alterado. Para verificar o certificado, o sistema operacional entra em contato com uma autoridade de certificação para verificar a identidade do editor do software. Esse é um comportamento normal para todos os programas assinados digitalmente no Microsoft Windows.

O que é a tecnologia Anti-Stealth?

A tecnologia Anti-Stealth proporciona a detecção efetiva de rootkits.

Se o sistema for atacado por um código malicioso que se comporte como um rootkit, o usuário poderá ser exposto à perda ou ao roubo de dados. Sem uma ferramenta especial anti-rootkit, é quase impossível detectar rootkits.

Por que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente ao mesmo tempo?

Ao tentar identificar a assinatura digital de um arquivo executável, o ESET SysInspector primeiro verifica se há uma assinatura digital incorporada no arquivo. Se uma assinatura digital for encontrada, o arquivo será validado usando essa informação. Se a assinatura digital não for encontrada, o ESI iniciará a procura do arquivo CAT (Security Catalog - *%systemroot%\system32\catroot*) correspondente que contenha informações sobre o arquivo executável processado.

Caso o arquivo CAT relevante seja encontrado, sua assinatura digital será aplicada no processo de validação do executável.

É por isso que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente.

Exemplo:

O Windows 2000 inclui o aplicativo HyperTerminal, localizado em *C:\Arquivos de Programas\Windows NT*. O arquivo executável principal do aplicativo não é assinado digitalmente, mas o ESET SysInspector o marca como um arquivo assinado pela Microsoft. O motivo disso é a referência em *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* que aponta para *C:\Program Files\Windows NT\hypertrm.exe* (o executável principal do aplicativo HyperTerminal) e o *sp4.cat* é digitalmente assinado pela Microsoft.

12. ESET SysRescue

o ESET SysRescue é um utilitário que permite a criação de um disco de inicialização contendo uma das soluções ESET Security, podendo ser o ESET NOD32 Antivirus, o ESET Smart Security ou até mesmo algum dos produtos orientados ao servidor. A principal vantagem do ESET SysRescue é o fato de que a solução ESET Security é executada de maneira independente do sistema operacional host, ao mesmo tempo em que possui um acesso direto ao disco e a todo o sistema de arquivos. Isso permite remover infiltrações que normalmente não poderiam ser excluídas, por exemplo, quando o sistema operacional está em execução, etc.

12.1 Requisitos mínimos

o ESET SysRescue funciona no Microsoft Windows Preinstallation Environment (Windows PE) versão 2.x, que é baseado no Windows Vista.

O Windows PE faz parte do pacote gratuito do Windows Automated Installation Kit (Windows AIK), portanto o Windows AIK deve ser instalado antes da criação do ESET SysRescue (http://go.eset.eu/AIK). Devido ao suporte da versão de 32 bits do Windows PE, é necessário usar o pacote de instalação de 32 bits da solução ESET Security ao criar o ESET SysRescue em sistemas de 64 bits. O ESET SysRescue é compatível com o Windows AIK 1.1 e versões posteriores.

OBSERVAÇÃO: Como o Windows AIK é maior que 1 GB, uma conexão com a Internet de alta velocidade é necessária para um download perfeito.

o ESET SysRescue está disponível nas soluções ESET Security 4.0 e versões posteriores.

Sistemas operacionais compatíveis

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 com KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 com KB926044
- Windows XP Service Pack 3

12.2 Como criar o CD de restauração

Para iniciar o assistente ESET SysRescue, clique em **Iniciar** > **Programas** > **ESET** > **ESET Remote Administrator** > **ESET SysRescue**.

Primeiro, o assistente verifica a presença do Windows AIK e de um dispositivo adequado para a criação da mídia de inicialização. Se o Windows AIK não estiver instalado no computador (ou estiver corrompido ou instalado incorretamente), o assistente dará a opção de instalá-lo ou de inserir o caminho para a pasta do Windows AIK (http://go.eset.eu/AIK).

OBSERVAÇÃO: Como o Windows AIK é maior que 1 GB, uma conexão com a Internet de alta velocidade é necessária para um download perfeito.

Na próxima etapa 153, selecione a mídia de destino em que o ESET SysRescue estará localizado.

12.3 Seleção de alvos

Além de CD/DVD/USB, você pode escolher salvar o ESET SysRescue em um arquivo ISO. Posteriormente, é possível gravar a imagem ISO em CD/DVD ou utilizá-la de alguma outra maneira (por exemplo, no ambiente virtual, como VMWare ou VirtualBox).

Se você selecionar USB como a mídia-alvo, a reinicialização pode não funcionar em determinados computadores. Algumas versões de BIOS podem relatar problemas com o BIOS - comunicação com o gerenciador de inicialização (por exemplo, no Windows Vista), e a inicialização é encerrada com a seguinte email de erro:

```
arquivo: \boot\bcd
status: 0xc000000e
informações: an error occurred while attemping to read the boot configuration data (ocorreu um erro ao tenta
```

Se você encontrar essa email, recomendamos que selecione o CD, em vez da mídia USB.

12.4 Configurações

Antes de iniciar a criação do ESET SysRescue, o assistente de instalação exibe os parâmetros de compilação na última etapa do assistente do ESET SysRescue. Para modificá-los, clique no botão **Alterar...**. As opções disponíveis incluem:

- Pastas 153
- Antivírus ESET 154
- Avançadas 154
- Protoc. Internet 154
- Dispositivo USB inicializável 154 (quando o dispositivo USB de destino é selecionado)
- Gravação 155 (quando a unidade de CD/DVD de destino é selecionada)

O botão **Criar** estará inativo se nenhum pacote de instalação MSI for especificado ou se nenhuma solução ESET Security estiver instalada no computador. Para selecionar um pacote de instalação, clique no botão **Alterar** e vá para a guia **Antivírus ESET**. Além disso, se você não preencher o nome do usuário e a senha (**Alterar** > **Antivírus ESET**), o botão **Criar** estará acinzentado.

12.4.1 Pastas

A **Pasta temporária** é um diretório de trabalho para arquivos exigidos durante a compilação do ESET SysRescue.

A pasta **ISO** é a pasta onde o arquivo ISO resultante é salvo após a conclusão da compilação.

A lista nessa guia mostra todas as unidades de rede locais e mapeadas, junto com o espaço livre disponível. Se algumas das pastas estiverem localizadas em uma unidade com espaço livre insuficiente, recomendamos que você selecione outra unidade com mais espaço livre disponível. Caso contrário, a compilação pode terminar prematuramente devido a espaço livre em disco insuficiente.

Aplicativos externos - Permite especificar os programas adicionais que serão executados ou instalados após a inicialização a partir de uma mídia do ESET SysRescue.

Incluir aplicativos externos - Permite adicionar programas externos à compilação do ESET SysRescue.

Pasta selecionada - Pasta na qual os programas a serem adicionados ao disco do ESET SysRescue estão localizados.

12.4.2 Antivírus ESET

Para criar o CD do ESET SysRescue, é possível selecionar duas fontes de arquivos da ESET para serem utilizadas pelo compilador.

Pasta do ESS/EAV - Arquivos já contidos na pasta na qual a solução ESET Security está instalada no computador.

Arquivo MSI - São usados os arquivos contidos no instalador do MSI.

Em seguida, é possível atualizar a localização dos arquivos (.nup). Normalmente, a opção padrão **Pasta do ESS/EAV/ Arquivo MSI** deve ser definida. Em alguns casos, uma **Pasta de atualização** personalizada pode ser definida, por exemplo, para usar uma versão mais antiga ou mais recente de um banco de dados de assinatura de vírus.

É possível utilizar uma das seguintes fontes de nome de usuário e senha:

ESS instalado - O nome de usuário e a senha são copiados da solução ESET Security instalada no momento.

Do usuário - O nome de usuário e a senha digitados nas caixas de texto correspondentes serão utilizados.

OBSERVAÇÃO: a solução ESET Security no CD do ESET SysRescue é atualizada a partir da Internet ou da solução ESET Security instalada no computador em que o CD do ESET SysRescue for executado.

12.4.3 Configurações avançadas

A guia **Avançado** permite otimizar o CD do ESET SysRescue de acordo com o tamanho da memória do computador. Selecione **576 MB ou mais** para gravar o conteúdo do CD na memória operacional (RAM). Se você selecionar **menos de 576 MB**, o CD de recuperação será permanentemente acessado quando o WinPE estiver em execução.

Na seção **Drivers externos** é possível inserir drivers para o seu hardware específico (geralmente o adaptador de rede). Embora o WinPE seja baseado no Windows Vista SP1, que suporta uma larga escala de hardware, algumas vezes o hardware não é reconhecido. Isso requer que o driver seja adicionado manualmente. Há duas maneiras de inserir o driver em uma compilação do ESET SysRescue - manualmente (botão **Adicionar**) e automaticamente (botão **Pesquisa Automática**). No caso de inclusão manual, é preciso selecionar o caminho para o arquivo .inf correspondente (o arquivo *.sys aplicável também deve estar presente nessa pasta). No caso de inserção automática, o driver é encontrado automaticamente no sistema operacional do computador específico. Recomendamos que use a inclusão automática apenas se o ESET SysRescue for usado em um computador com o mesmo adaptador de rede usado no computador em que o CD ESET SysRescue foi criado. Durante a criação, o driver do ESET SysRescue é inserido na compilação para que você não precise procurá-lo depois.

12.4.4 Protoc. Internet

Essa seção permite configurar informações básicas de rede e definir as conexões predefinidas após o ESET SysRescue.

Selecione **Endereço IP privado autom.** para obter o endereço IP automaticamente a partir do servidor DHCP (Dynamic Host Configuration Protocol, protocolo de configuração dinâmica de endereços de rede).

Se preferir, a conexão de rede pode usar um endereço IP especificado manualmente (também conhecido como endereço IP estático). Selecione **Personalizar** para definir as configurações adequadas para o endereço IP. Ao definir essa opção, é preciso especificar um **Endereço IP** e, para a LAN e as conexões de Internet de alta velocidade, uma **Máscara de sub-rede**. Em **Servidor DNS preferencial** e **Servidor DNS alternativo**, digite os endereços principal e secundário do servidor DNS.

12.4.5 Dispositivo USB inicializável

Se você selecionou um dispositivo USB como mídia-alvo, é possível selecionar um dos dispositivos USB disponíveis na guia **Dispositivo USB inicializável** (caso haja mais dispositivos USB).

Selecione o **Dispositivo** de destino apropriado onde o ESET SysRescue será instalado.

Aviso: O dispositivo USB selecionado será formatado durante a criação do ESET SysRescue. Todos os dados no dispositivo serão excluídos.

Se você optar por uma **Formatação rápida**, a formatação removerá todos os arquivos da partição, mas não rastreará o disco em busca de setores corrompidos. Use essa opção se o dispositivo USB tiver sido formatado anteriormente e você tiver certeza de que ele não está danificado.

12.4.6 Gravar

Se você selecionou CD/DVD como sua mídia-alvo, é possível especificar parâmetros de gravação adicionais na guia **Gravar**.

Excluir arquivo ISO - Marque essa opção para excluir o arquivo ISO temporário após o CD do ESET SysRescue ser criado.

Exclusão ativada - Permite selecionar o apagamento rápido e concluí-lo.

Dispositivo de gravação - Selecione a unidade a ser utilizada para gravação.

Aviso: Essa é a opção padrão. Se um CD/DVD regravável for usado, todos os dados contidos no CD/DVD serão apagados.

A seção Mídia contém informações sobre a mídia no seu dispositivo de CD/DVD.

Velocidade de gravação - Selecione a velocidade desejada no menu suspenso. Os recursos do seu dispositivo de gravação e o tipo de CD/DVD utilizado devem ser considerados ao selecionar a velocidade da gravação.

12.5 Trabalhar com o ESET SysRescue

Para o CD/DVD/USB de restauração funcionar de forma eficiente, é necessário que o computador seja inicializado a partir da mídia de inicialização do ESET SysRescue. A prioridade de inicialização pode ser modificada no BIOS. Como alternativa, você pode usar o menu de inicialização durante a inicialização do computador, geralmente utilizando uma das teclas: F9 a F12, dependendo da versão da placa-mãe/do BIOS.

Após a inicialização da mídia de inicialização, a solução ESET Security será iniciada. Como o ESET SysRescue é utilizado apenas em situações específicas, alguns módulos de proteção e recursos do programa presentes na versão padrão da solução ESET Security não são necessários; a lista é limitada ao **Rastrear o computador**, à opção **Atualizar**, e algumas seções da **Configuração**. A capacidade de atualizar o banco de dados de assinaturas de vírus é o recurso mais importante do ESET SysRescue. Recomendamos que você atualize o programa antes de iniciar um rastrear o computador.

12.5.1 Utilização do ESET SysRescue

Suponha que os computadores na rede tenham sido infectados por um vírus que modifica os arquivos executáveis (. exe). A solução ESET Security consegue limpar todos os arquivos infectados, exceto o *explorer.exe*, que não pode ser limpo, mesmo no modo de segurança. Isso ocorre porque o *explorer.exe*, como um dos processos essenciais do Windows, também é iniciado no modo de segurança. A solução ESET Security não poderia realizar ações com o arquivo e ele permaneceria infectado.

Nesse tipo de cenário, seria possível usar o ESET SysRescue para solucionar o problema. O ESET SysRescue não requer componentes do sistema operacional host, portanto ele pode processar (limpar, excluir) qualquer arquivo no disco.

13. Apêndice - Licença de terceiros

A ESET reconhece que o Software inclui código de terceiros, que está sujeito a estas licenças de terceiros:

3-clause BSD License ("New BSD License")

Copyright (c) <YEAR>, <OWNER>
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
• Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
• Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
• Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>
Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>
Copyright (c) 2006-2007 The Written Word, Inc.
Copyright (c) 2007 Eli Fant <elifantu@mail.ru>
Copyright (c) 2009 Daniel Stenberg
Copyright (C) 2008, 2009 Simon Josefsson
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
• Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
• Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
• Neither the name of the copyright holder nor the names of any other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."